International Journal of Information Security (2023) 22:1799–1832
https://doi.org/10.1007/s10207-023-00720-z

REGULAR CONTRIBUTION

A survey of anomaly detection methods for power grids

Srinidhi Madabhushi[1] · **Rinku Dewri**[1]

Published online: 8 July 2023

Abstract
The power grid is a constant target for attacks as they have the potential to affect a large geographical location, thus affecting hundreds of thousands of customers. With the advent of wireless sensor networks in the smart grids, the distributed network has more vulnerabilities than before, giving numerous entry points for an attacker. The power grid operation is usually not hindered by small-scale attacks; it is popularly known to be self-healing and recovers from an attack as the neighboring areas can mitigate the loss and prevent cascading failures. However, the attackers could target users, admins and other control personnel, disabling access to their systems and causing a delay in the required action to be taken. Termed as the biggest machine in the world, the US power grid has only been having an increased risk of outages due to cyber attacks. This work focuses on structuring the attack detection literature in power grids and provides a systematic review and insights into the work done in the past decade in the area of anomaly or attack detection in the domain.

Keywords Attack detection · Anomaly detection · Intrusion detection system · Cyber physical system · Power grid · Smart grid

1 Introduction

The power system is one of the most critical infrastructures in modern society. It has been a target for cyber and physical attacks in the past two decades. It has many components that depend on each other and work in a coordinated manner for seamless operation. Hence, when any major component fails to operate, it causes cascading effects on the other components as well. For better monitoring and security, smart meters, sensors and IoT devices are being integrated. An objective of the so-called "smart grid" is to use more information in a smarter way to optimize power systems [107]. Security is one of the important challenges in cyber-physical systems due to this integration which has made them vulnerable on both the physical and cyber sides [124]. With different attacks that have occurred and have been recognized, anomaly or intrusion detection systems are now in demand in the power domain [9]. Anomaly detection systems (ADS) are used to identify events or observations that seem suspicious when compared to the normal behavior of the data.

In this survey, we review a collection of 190 papers covering the power grid architecture, its vulnerable points, and primarily, the range of anomaly detection techniques that have been proposed in the domain to detect exploits. The systematization led us to a range of challenges that are promising avenues for future research to enhance the efficacy of anomaly detection methods while aiding traditional attack detection and response platforms.

Figure 1 shows an overview of this survey's organization. We begin in Sect. 2 with a discussion of the methodology for carrying out the systematization of knowledge. We then provide relevant background information in Sect. 3, regarding the power grid architecture and its processes (Sect. 3.1), the different attack types and targets in the power grid (Sect. 3.2), and the different locations in the power grid where anomaly detection can be applied, as well as the types of anomalies that can be detected (Sect. 3.3). Next, we motivate the need for detection methods in Sect. 4, by discussing some of the past attacks that have taken place (Sect. 4.1), the new demand manipulation attack (MAD) and how they can be carried out using IoT devices (Sect. 4.2), and lastly the attack impact on the power grid (Sect. 4.3). We then dive deeper into the anomaly detection methods proposed for the power grid and

✉ Rinku Dewri
rdewri@cs.du.edu

Srinidhi Madabhushi
nidhi.madabhushi@du.edu

[1] University of Denver, Denver, CO, USA

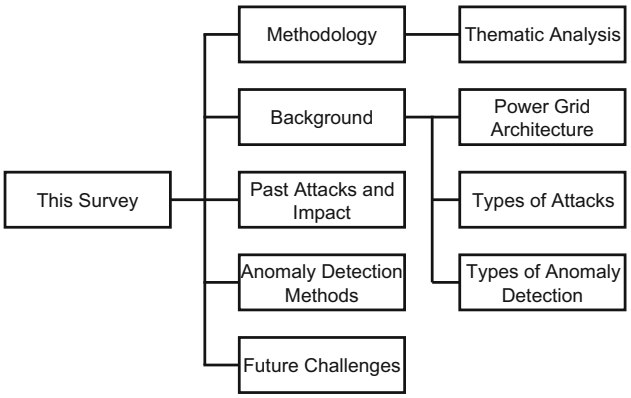

Fig. 1 Overview of the organization in this survey

discuss the various methods identified in the literature in Sect. 5. Next, in Sect. 6, we discuss the current challenges in the area of anomaly detection in power grids, and highlight potential future directions of research. Lastly, we conclude the paper in Sect. 7.

1.1 Related work and contribution

In this work, we focus on assimilating the different types of anomaly detection methods used in the power grid in a single place. One of the most comprehensive surveys on anomaly detection was done by Chandola et al. which focuses on all types of detection techniques applied to any application domain [29]. Cyber security for smart grid infrastructure and the issues in the smart grid are discussed in [10] and [226]. There are several open threats and attacks on the smart grid that have been identified, with potential solutions including access control, security of network protocols and attack detection methods [67, 94, 98, 148]. With the increasing usage of IoT devices for collecting readings and monitoring the grid states, the security of the smart grid that is aided by IoT devices is discussed in [172].

The papers that focus on surveying or reviewing various detection techniques in the power grid context are done either by choosing a single technique or a single power grid application. For example, some surveys focus on detection techniques for consumption data [56, 73], multimodal image data [241] or for time series data in the smart grids [233], whereas we consider any type of data. Mohammadi Rouzbahani et al. focus on machine learning techniques for detection in cyber-physical systems [56]; we consider any kind of detection technique that may be statistical, rule-based, or graph-based, among others. Unlike in [190], where the thematic analysis is carried out on process data and features considered for detection, we also consider the paper type, power grid application, attack type and detection types. We show a comparison of this survey with similar existing surveys in the last five years in Table 1. While reviews and

Table 1 Comparison of this survey with existing survey papers in the last five years

Criteria	This survey (2023)	Sahani et al. [170]	Alkuwari et al. [8]	Himeur et al. [73]	Haque et al. [69]	Wang et al. [204]	Hu et al. [78]
Timeline of literature	2009–2023	2002–2022	2012–2022	2000–2021	2011–2020	2011–2017	1997–2018
Power Grid Application	Any	SCADA, WSN, AMI	Transmission, Distribution, AMI	Buildings	Transmission, AMI, Networks	Any	SCADA, Networks
Type of Attacks for Detection	Any	Cyber	Cyber, Physical	Anomalous consumption	Cyber	Cyber, Physical	Cyber
Type of Detection Methods	Any	Supervised, Unsupervised	Any	Any	Supervised, Unsupervised	Supervised, Unsupervised	Supervised, Unsupervised
Future Research Challenges	●	●	○	●	◐	◐	◐
Detailed Thematic Analysis	●	◐	◐	◐	◐	○	◐

● Surveyed and classified, ◐ Partially addressed, ○ Neither surveyed nor classified

surveys have been published in this area, this is the first paper to our knowledge that includes a comprehensive review of detection methods across the entire power grid considering different types of data. To this end, our main contributions in this work are as follows: (i) provide an overview across different themes that are identified during the systematic review, (ii) provide a detailed taxonomy of different detection techniques used in the power grid domain, and (iii) point out the gaps and challenges that currently exist in this domain.

2 Methodology

The research works used in this review are obtained and organized through a four-step process: (i) database search, (ii) title screening, (iii) abstract screening and (iv) thematic analysis. In this section, we discuss the methodology in detail.

2.1 Database and keyword search

We search through Google Scholar for three key phrases and obtain the first 100 results for each. The key phrases used are (i) *"anomaly detection power consumption"*, (ii) *"anomaly detection power grid"*, and (iii) *"anomaly detection smart grid"*. We select the option to sort by relevance and to obtain papers from any time range. At the end of this search, we get 300 papers that include work in progress (WiP), journal articles and conference papers. There are 50 unique papers that occurred multiple times in different keyword searches which are merged into a single version. After removing the duplicates, 238 papers remained for the next step of the analysis.

2.2 Inclusion and exclusion criteria

The selection criteria that are applied to the 238 papers are: (i) the paper should be related to any of the power grid processes, (ii) the paper should include anomaly detection or attack detection approaches in the power grid, (iii) the full text should be available through institutional access to the published conferences, journals or workshops, and (iv) the paper is not a WiP work. First, a title screening is done based on these criteria, after which 23 papers are excluded. Next, a thorough abstract screening is performed after which 21 papers are excluded. There are 4 papers that we cannot view through institutional access. A total of 48 papers are excluded leaving us with 190 papers for the analysis.

2.3 Thematic analysis

We follow a deductive approach to perform the thematic analysis and use a list of preconceived themes to find the codes in each theme. The themes, sub-themes and codes are listed in Table 2. The themes are identified before starting the analysis to categorize each paper with a code from every theme. There are 95 codes that are created. Once the codes are finalized, sub-themes are identified to provide a hierarchical view of the different types of codes that are observed. The codes are further divided into sub-codes specifically for the "Detection technique" theme, where each sub-code represents the method used. This is covered in detail in Sect. 5 with a taxonomy of methods identified. In this section, we discuss about the themes and sub-themes. The number of papers categorized into a single sub-theme is given in Table 2. The list of works under a specific code is available in Table 3.

2.3.1 Paper type

The `Paper Type` theme is used to recognize what type of research is conducted in every paper. This theme consists of five sub-themes that are mutually exclusive. A `Review`, `Survey` and `Evaluation` types include papers that conducted a thorough review, survey or evaluation of existing detection techniques that may be focused on a single area such as machine learning techniques, deep learning algorithms, techniques used for power consumption data, or communication network data. Papers that propose a new method or variation of existing methods to solve a detection problem in any power grid application are themed under `Methodology` type. A `Framework` sub-theme is where a paper proposes a new architecture that may not be necessarily implemented.

Within the `Methodology` sub-theme, the code `feature handling` is for papers that focus on treatment and extraction of features from the raw data for anomaly detection [174], `big data` is for techniques that are proposed for big data applications and `visual analysis` is for methods that focus on detection using visualization techniques.

2.3.2 Focus area

The `Focus Area` theme is for recognizing the area of contribution of the paper in the power grid domain. A paper may be categorized into multiple focus areas based on the proposed methodology. `Targeted Detection` is used to categorize papers that are focused on contributing a detection technique while optionally considering other aspects like concept drift, early detection, collective and contextual anomalies that may improve the detection process. When papers consider distributed computing and other edge detection concepts, we categorize them into `Big Data` and distributed computing sub-themes. As the names suggest, `Profiling` and `Privacy` sub-themes are for papers that analyze behavior profiles and propose privacy-preserving techniques respectively. `Wide Area Protection` is used to represent research that applies to

Table 2 Summary of themes, sub-themes, paper count per sub-theme and codes identified in this work; Table 3 provides the list of works under a specific code

Theme	Sub-theme	Count	Codes
Paper type	Review	5	review
	Survey	8	survey
	Methodology	130	new method, new methodology, feature handling, visual analysis, big data
	Framework	12	framework, architecture
	Evaluation	23	evaluation
Focus area	Targeted Detection	139	detection, drift, transfer learning, early detection, contextual, optimization, efficiency
	Big Data	24	cloud computing, fog computing, federated learning, edge detection, data-driven
	Profiling	5	behavior analysis
	Privacy	6	privacy-preserving
	Wide area protection	7	wide sensor network, sensor placement
	Blockchain	3	blockchain
Data type	Single Feature	145	consumption, network, voltage, current, frequency, sensors
	Multiple Features	27	system logs, weather, operational
	Visual	2	image
Grid process	Generation	6	generator, power plant, solar plant, wind turbine
	Transmission	18	transmission lines, transmission buses, substation, transmission sensors
	Distribution	28	distribution lines, DERs, distribution sensors, substation, power line modems
	Utility	80	AMI, building, commercial, edge devices, industrial, residential, smart home, smart meter
	Other	34	control software, grid sensors, scada
Attack type	Attack	65	brute force, coordinated, DDoS, DoS, insider, operational, network, intrusion, FDI, tripping lines, trojan, electricity theft, demand manipulation, zero day
	Other Anomalies	95	fault detection, anomalous behavior, anomalous usage, monitoring
Detection	Supervised	39	classification, neural network
	Semi-supervised	48	regression, statistical, distance-based, neural network, rule-based
	Unsupervised	69	clustering, neural network, nearest neighbor, OC classification, tree-based
	Other Techniques	11	fuzzy learning, reinforcement learning, graph-based

multiple sensors that are located across different power grid processes. Lastly, `Blockchain` is used to identify works that utilize blockchain technology for detection.

2.3.3 Data type

Different types of data features are used for the detection system based on the application in the power grid. This theme is used to categorize the papers based on the type of data that is used for the detection process. Generally, streaming data of a single device is used to detect anomalous behavior, but multiple features may also be used for identifying anomalous behavior that can be recognized with specific states of the different features. Additionally, images may also be used to monitor and identify faults using video data.

2.3.4 Power grid process

We categorize the detection methods based on the application location in the power grid. There are four main processes

in the power grid, namely `Generation`, `Transmission`, `Distribution` and `Utility`. Any detection method that does not apply to any of the four processes is themed into `Other` that consists of detection in energy management systems (EMS), software, sensors and supervisory control and data acquisition (SCADA). Within each of the power grid processes, we identify which devices are used for the detection mechanism to categorize them into their respective code.

2.3.5 Attack type

The papers here are categorized by the attack type that the detection system is targeted to identify. These attacks can be performed by an adversary or can be operational faults and unknown anomalous behavior. The codes for the attack types are shown in Table 2 and denote the attack names.

2.3.6 Detection

The `Detection` theme is used to categorize the paper based on the type of detection that is carried out. This can be supervised, semi-supervised, unsupervised or any other category that is not covered by the previous three. The codes specify what type of method is used for the detection process. The details about each of the detection techniques are covered in Sect. 5. A single research paper may have multiple detection techniques going across sub-themes as well. The list of works utilizing a specific detection technique is available in Table 4.

3 Background

In this section, we discuss the power grid architecture, attack targets in the power grid, and potential application points of anomaly detection at different areas in the power grid.

3.1 Power grid architecture

The power grid is a complex and highly engineered network that coordinates between the generation and distribution of electricity to its customers. Modern power systems have grown into a sophisticated cyber-physical system due to the expansion of their electrical infrastructure and the consequential application of diverse communication and information protocols. The modern power grid consists of two tightly coupled layers: physical and cyber layers. The physical layer is responsible for carrying electricity end-to-end and is the core of the power system. It consists of four major domains: generation, transmission, distribution and consumption, as shown in Fig. 2. Electric power is produced at the generating station and is then transmitted through a high voltage transmission network. From there, it is distributed to the end users which can be industrial or residential customers.

Over the years, power systems have become more heterogeneous in terms of all these domains. There have been major upgrades such as renewable energy plants, microgrids, and electricity storage. This brings great challenges for the operation of the power system to coordinate between different system components. Hence, efficient schemes are incorporated in the cyber layer that are responsible for ensuring security, protection and monitoring of the power grid.

The cyber layer consists of secondary devices and schemes that are capable of communication, data collection, storage, processing, and decision-making. For modern power systems, there are three most critical cyber layer systems: Supervisory Control and Data Acquisition (SCADA), wide area measurement system (WAMS) and advanced metering infrastructure (AMI). A remote terminal unit (RTU) is used to merge data from local secondary devices like sensors and meters. SCADA systems are industrial control systems responsible for distributed monitoring, control, collection and analysis of real-time data from RTUs. WAMS is an alternative to SCADA which collects data at a higher sampling rate from the phasor measurement units (PMUs), which measure and estimate the voltage, current magnitudes and relative phase angles. AMI is a system that is placed in the distribution sector that monitors, collects and analyzes the energy usage data of consumers. A large number of smart meters are deployed to collect real-time energy usage data to derive appropriate demand side control for reliable operations [205].

The smart grid network architecture includes Home Area Network (HAN), Neighborhood Area Network (NAN) and Wide Area Network (WAN) [224]. HAN and NAN are used by the Advanced Metering Infrastructure that includes smart meters, data concentrators and other metering components. Customers can also access their consumption portal using the HAN. NAN is built over the HAN and ensures communication between HANs, data centers and generation sources. On the other hand, WAN is used by wide area monitoring and controlling applications like SCADA and WAMS with limited bandwidth and capacity in closed networks.

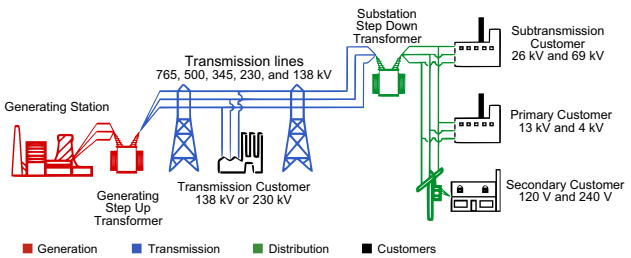

Fig. 2 Physical layer of the power grid; reproduced from [214] under CC BY 3.0

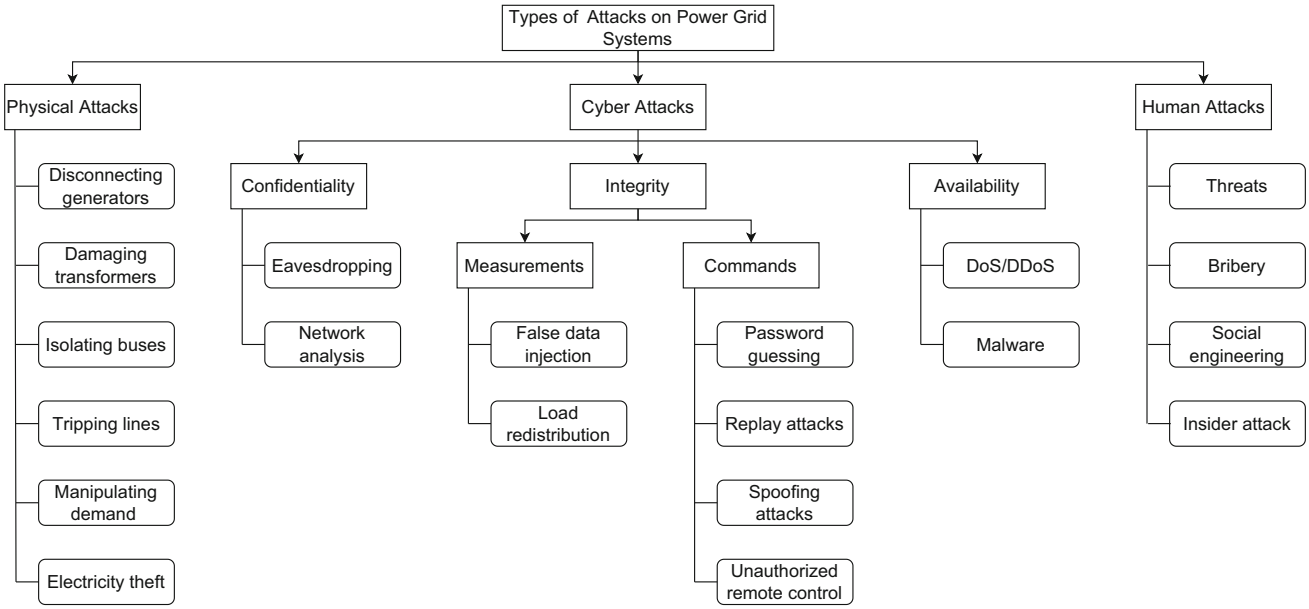

Fig. 3 Types of attacks on the power grid

3.2 Attack targets

Attacks can be targeted either towards the physical layer or the cyber layer. It is possible that there can be attacks on humans, such as on power system personnel, or even performed by them due to threats or bribery from attackers. We have three types of attacks on the power grid: physical attacks, cyber attacks and human attacks. Fig. 3 summarizes the different attacks possible on a power grid.

3.2.1 Physical attacks

Physical attacks are targeted at the physical components of the power grid. These attacks can be performed in any power grid domain, i.e. generation, transmission, or distribution. The generation process can be affected when an adversary disconnects the generators by remotely switching them off, removing any supporting cords from outlets or hindering the connection between the generator and other supporting devices. A transformer failure can occur by lightning strikes, degradation of any electrical insulation, power overload or direct incursion on the transformer. An adversary can hinder the tasks of current-carrying devices in the field that causes tripping of lines or can steal energy by doing so. Lastly, an adversary can manipulate the demand by controlling the consumers' devices which can result in a chain reaction of the above physical attacks.

3.2.2 Cyber attacks

Cyber attacks are classified based on the basic requirements of a general cyber network into attacks against availability, integrity and confidentiality. An attack against availability can cause the loss of control of the local devices or a delayed response. For example, an attacker can affect the communication network by launching a DoS attack and hence, cause a delay of operation commands sent to local devices or the measurements sent to the control center. Injecting malware into the network can also affect the availability of the system by taking it offline or damaging existing files. An attack against confidentiality can cause the leakage of critical information. SCADA devices comprise remote terminal units (RTUs), programmable logic controllers (PLCs) and intelligent electronic devices (IEDs) which do not incorporate authentication or encryption mechanisms and hence, are at high risk of being exploited. Also, DNP3 is used by most North American utilities as a communication protocol, which still lacks security features like encryption or authentication. Due to these existing vulnerabilities, an adversary can get access to a device or the network and can analyze the traffic packets and information exchanged on the network. An attack against integrity can compromise the data and information communication in the cyber network, which can severely affect the normal operation of the power grid. While all the cyber attacks have negative impacts on the power grid, the attacks against integrity would be relatively more severe. Thus, it is further divided into attacks against measurements and attacks against commands. The attacker can manipulate a set of measurements to change the state estimation

outcome and mislead the operator to make non-optimal or wrong dispatch decisions. This is achieved by either altering sensor data leading to a false data injection attack or by injecting false measurements in transmission and distribution buses leading to a load redistribution attack. Fabricated control commands may be sent to power grid devices to hinder its operation. This can be achieved by guessing passwords to control systems, replaying network traffic messages to perform specific actions, spoofing attacks and unauthorized access to remote devices.

3.2.3 Human attacks

Human attacks occur when a power grid associated personnel intentionally or unintentionally leak critical information or are forced to take some detrimental actions. It can also be possible that some consumers are misguided to perform an action such as switching on or off the devices in their houses, through false alerts sent to their phones. Such actions are difficult to prevent and affect the power grid operation with a huge impact.

3.2.4 Coordinated attacks

Coordinated attacks involve multiple attacks at the same time or a combination of any of the above three categories of attacks to cause severe failure, thus having a high attack success rate. For example, there can be coordinated physical attacks on multiple lines, coordinated cyber attacks against multiple substations or physically tripping a line and performing a DDoS attack in the SCADA network to produce a delayed operator's response that may all lead to a severe failure [218]. A coordinated attack was performed during the 2015 cyber attack on the Ukrainian power grid attack (detailed in the next section).

3.3 Anomaly detection

Anomaly detection refers to the problem of finding patterns in data that do not conform to expected behaviour [29]. In the power grid domain, anomaly detection is applied to a variety of tasks like finding abnormal consumption behaviors, identifying compromised field devices, anomalous grid states, line overloads, and attack detection. These techniques vary based on the applied area or objective of the detection. Figure 4 shows the different types of detection systems that are applied based on the detection area in the grid [66, 205]. This model does not imply the application of a detection technique at a physical location. This distinction is made to understand different types of views that can be combined by the grid operator for the detection of different anomalous instances in power systems. We will discuss each of these types and the assumed threat models.

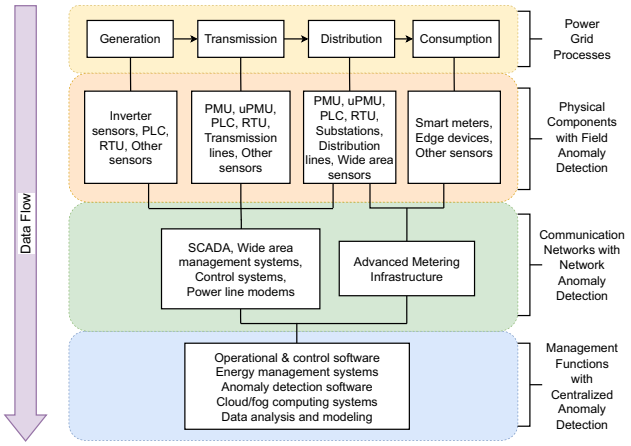

Fig. 4 Abstract architecture of a power grid with possible applications of anomaly detection at different levels of data flow

3.3.1 Field anomaly detection

Field anomaly detection focuses on the field components that are important for running the power grid. Based on the area of the physical components placed in any of the power grid essential processes, the components may differ based on their functionality. In the following, we discuss the different components that require anomaly and/or intrusion detection systems and list the types of attacks that are expected to be detected by such a system.

The Remote Terminal Units (RTUs) are used to interface the different physical components mainly, Intelligent Electronic Devices (IEDs) which include transformers, PLCs and circuit breakers, to the SCADA master station. It transmits the data collected from these devices to a data collection system using different communication protocols that can be serial or Ethernet-based. Phasor Measurement Units (PMUs) are devices that measure and report phasor angle and magnitude for the AC voltage or current at a specific location on a power line. These measurements are used for monitoring and analysis of the grid states. These values facilitate improving the accuracies of modeling system conditions, predicting and detecting stress and instability of the grid, predicting and managing line congestion and identifying any field inefficiencies. PMUs are used to replace the traditional SCADA devices with the benefit that they can provide up to 60 measurements a second compared to one in every 2 to 4 s [53]. Phasor Data Concentrators (PDCs) are used for collecting data from different PMUs, aggregate and time synchronize data and send it to synchrophasor applications that use the data [135]. Smart meters are used in distribution and consumption processes that record information like voltage, current, consumption and power factor. They communicate this information to the consumers for greater clarity of con-

sumption behavior, as well as electric suppliers for system monitoring and customer billing.

We can see that all these devices that are used in different stages from electricity generation to delivery, have an important role in the reliable transmission and delivery of electricity from end to end. As these devices are crucial for the collection of information required for estimation, operation and monitoring, the data coming from these devices can be altered by an attacker, thus affecting the integrity of the data. Therefore, the detection task in this category is to identify bad measurements and compromised devices at the field level by using the normal behavior patterns of these devices when not under attack.

Threat In SCADA systems, the PLCs are used to manage specific equipment and to run automation tasks in the power grid and hence, are a common target to the attackers. As PLCs are light weight devices that run a specific task based on the code they run, attackers take advantage of these devices with less security and change the code to do any malicious tasks. One such attack was accomplished by using the Stuxnet worm (discussed in Sect. 4.1.1). IEDs, which are used to manage automation tasks in the power grid, can also be manipulated similarly. There are inherent vulnerabilities in encryption and authentication mechanisms of RTUs and PMUs which is a threat that the attackers often use to perform False Data Injection (FDI) attacks. FDI attacks aiming at the physical layer give attackers the power to change the measurements of these devices transmitted to the monitoring systems. This will result in disruption of the analysis results of state estimation, leading to the control center misjudging the power grid into emergency and implementing maloperation, thus damaging the economic benefits, monitoring capability and safe operation of the power system [207].

Types of attacks that can be detected False data injection attacks, load redistribution attacks, demand manipulation attacks.

3.3.2 Network anomaly detection

Communication networks are used by SCADA, WAMS and AMI to obtain data from the physical components and transfer to management and control centers. Denial of service attacks (DoS) are the most common attacks used by intruders in a network. In fact, a DoS attack was one of many attacks performed in a coordinated manner during the 2016 attack on the Ukrainian power grid. The SCADA communication networks are increasingly interconnected with corporate information technology (IT) networks for the collection and processing of data in real-time, thus providing greater opportunities for intrusion [144]. With the advent of WAMS and AMI, there are numerous devices and sensors connected to this communication network and hence, there is a higher chance of intrusion. Since the monitoring systems have the permissions to change the control codes or the behavior of the physical devices, this is a very critical layer in the power grid operations. With AMI, the privacy of the data collected from Smart Meters can also be compromised. Hence, conventional cyber intrusion detection systems can be applied in the networking environment.

Threat There can be intrusions into the network by attackers that can stay undetected for a while to gain information about the grid operations, obtain the data from the monitoring systems, lock the power systems personnel out of their systems, password guessing, replay and spoofing attacks, reprogramming or sending false commands to the underlying devices, or sending incorrect information to the management centers.

Types of attacks that can be detected Insider attacks, intrusion attacks, replay attacks, spoofing attacks, DoS/DDoS attacks, information theft.

3.3.3 Centralized anomaly detection

Control and management centers receive the data that has been collected from the physical components and also have access to global system features. Hence, anomaly detection can utilize numerous features to find general anomalous system behavior, consumption demands from the consumers and bad data measurements from the physical devices. This layer uses a combination of both field and network detection systems, but gives a centralized view of the entire power system to take control decisions. This layer aids in the detection of coordinated attacks on the power grid. Though such attacks are challenging to detect in practice, there is a possibility to detect these attacks by analyzing multiple layers at the same time using the centralized view.

Threat It is a combination of field and network threats and are required to be analyzed together.

Types of attacks that can be detected Coordinated attacks.

4 Attacks and impact

There have been numerous attacks in the past decade targeting the power grid. The goal of attacks that have taken place is not just to disrupt the power grid but also to steal electricity and access confidential documents from the communication networks. Other attacks are possible, such as false data injection attacks, which disrupt the grid system state estimation. In 2014, the adversary stole and posted plans for two nuclear reactors, as well as the data of 10,000 employees from a South Korean nuclear and hydroelectric company Korea Hydro and Nuclear Power (KHNP). The Ukrainian power grid was taken down by the adversary, cutting power to more than 200,000 households in 2015. It was attacked again in 2016 by disabling an electricity substation, cutting power for an hour to the customers. In 2019, the US Power grid was attacked for

a 10-hour period where the attacker(s) exploited known vulnerabilities in an internet-connected firewall [198]. The US Department of Energy (DoE) reported 150 successful attacks between 2010 and 2014 that targeted systems holding information regarding electricity grids [110].

SCADA workstations and PLCs have also been a target for successful attacks on industrial control systems that use these components [35, 119]. There have been attacks involving the Stuxnet worm which sabotages industrial equipment controlled by a specific Siemens PLC by modifying PLC code and then hiding changes using rootkits. Such worms can cause severe damage to the underlying physical system [144].

The failure of a power grid can cause direct permanent effects on the equipment. It also results in failure of operation of other infrastructure as well. Hence, security of the power grid has been popular among researchers to address vulnerabilities and propose new mechanisms to detect intrusions. We discuss attacks that took place in the past and also some that are newly proposed which is the motivation behind creating new anomaly and attack detection methods. Figure 5 shows an overview of the attacks discussed in this section.

4.1 Past attacks

In this section, we discuss two cyber attacks that took down targeted critical infrastructure in 2010 and 2015. These attacks were initiated through computers targeted to affect the physical components of the infrastructure.

4.1.1 Stuxnet worm attack

Computer worms are well known to spread to many targets as quickly as possible. They are aimed at computer systems to exploit vulnerabilities, like Blaster which exploited the remote procedure call (RPC) of Windows computers. Some were used to physically impact the system, like Sobig which flooded mail servers with copies of itself [32]. However, a new worm was discovered by VirusBlokAda in Iran's nuclear

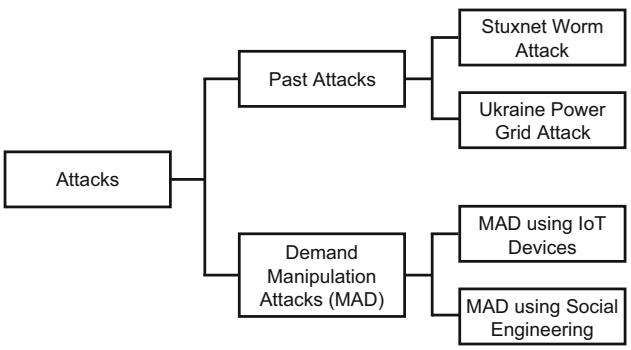

Fig. 5 Overview of the attacks discussed in Sect. 4

power plant in July 2010 called the Stuxnet. Unlike traditional worms which targeted computer systems, Stuxnet was developed to take control of critical physical infrastructure. It is known to have infected approximately 100,000 hosts, with more than 60,000 in Iran and more than 20,000 in Indonesia, India and the USA according to a Symantec's report [55]. This worm gained a lot of attention due to the stealth of the attack, and is known to have been one of the most complex threats. The following were the steps carried out to perform the attack using Stuxnet [55]:

- The attackers conducted reconnaissance; as each PLC is configured uniquely, they would first need the Industrial Control System (ICS) schematics. The documents required to attain knowledge of the computing environment in the facility were either stolen by an insider or retrieved by any other previous version of Stuxnet or other malicious binary.
- Using the information attained, the attackers would now develop the latest version of Stuxnet with the final goal of potentially sabotaging the ICS.
- Once the code is ready, the attackers probably used a setup mirroring the target environment to successfully test the code.
- As the malicious binaries consisted of driver files that were needed to be digitally signed, they compromised two digital certificates to achieve this task and appear legitimate.
- The initial infection vector is a USB stick to infect a computer within the organization. This USB keeps count and allows only three infections. This was introduced into the target perhaps by a compromised personnel who had access to the facility. The infection running on a target system attempts to spread only for 21 days. These limits were enforced perhaps to maintain the stealth of the attack [32].
- As soon as a single computer is infected, it searches for other Field PGs, copies and executes itself on computers running a WinCC database server. Field PGs are computers used to program or interact with the PLCs and are typically Windows systems. Most of these computers are non-networked and hence, cannot be remotely controlled using the Internet. Hence, Stuxnet would first try to spread on the LAN through a zero-day vulnerability that allowed infecting Step 7 projects through removable devices. WinCC/Step 7 software is used by the programmers to connect to the PLC and access the memory contents, reconfigure it, download or debug a program.
- All the functionality required to sabotage a system was directly embedded in the Stuxnet executable and hence, was complex and large for a malware being almost half a megabyte written in multiple languages. Once it found

a suitable computer that ran Step 7, it would then modify the code on the PLC. These modifications could not be detected as rogue PLC code as Stuxnet hides them using a rootkit.

4.1.2 Ukraine power grid attack

On December 23, 2015, a Ukrainian regional electricity distribution company reported outages to customers. The outages were due to a third party's illegal entry into the company's computer and SCADA systems. Approximately 225,000 customers were affected and lost power due to this incident. Three Ukrainian power suppliers experienced coordinated cyber attacks that were executed within 30 min of each other. Due to the large-scale impact, the suppliers were required to move to manual operations in response to the attack. Several consolidated technical components were used to successfully perform the attack. These are the steps carried out to perform the attack [26]:

- The attack phases are explained by using the Industrial Control System (ICS) Cyber Kill Chain, which details the steps an adversary must follow to perform high-confidence attack on the ICS processes and cause physical damage to equipment in a predictable and controllable way. It consists of two stages: intrusion and attack.
- The attacker was able to successfully intrude into the system by weaponizing Microsoft Office documents embedded with BlackEnergy 3 within the documents. These documents were sent out by email. When these documents were opened, a popup was displayed to users to encourage them to enable macros which allowed the malware to exploit the macro functionality to install BlackEnergy 3 on the victim's system.
- Upon installation, the malware connected to command and control (C2) IP addresses to enable communication by the adversary with the malware and the infected systems. These pathways allowed the adversary to gather information from the environment and enable access. They were also able to gain access to the remainder of the systems including the SCADA dispatch workstations and servers and extract data necessary to formulate a plan for the second stage (ICS attack).
- For the second stage, the attackers learned how to interact with the distribution management system environments using the native control present in the system and operator screens. The adversary completed installing malicious software which was identified as a modified version of KillDisk across the environment.
- The last act of modification was for the adversaries to take control of the operator workstations and thereby lock the operators out of their systems. The adversaries used the Human Machine Interfaces (HMIs) in the SCADA environment to open the breakers. At least 27 substations were taken offline across the three energy companies, impacting roughly 225,000 customers.
- Simultaneously, the attackers uploaded the malicious firm-ware to the serial-to-ethernet gateway devices. This ensured that even if the operator workstations were recovered, remote commands could not be issued to bring the substations back online.
- During this same period, the attackers also leveraged a remote telephonic denial of service on the energy company's call center with thousands of calls to ensure that impacted customers could not report outages.

4.2 Demand manipulation attacks

While smart grids are often known to be vulnerable to cyber attacks compared to traditional power grids, Dabrowski et al. show how a non-smart grid is also vulnerable to coordinated load changing attacks [41]. This attack is performed by controlling a botnet of devices that can modulate the power demand much faster than power plants can react. Demand manipulation attacks take place at the utility side, where an attacker can manipulate the consumption and operation of the consumer devices, mostly being IoT devices that can be remotely controlled [187]. The attacker can also influence the behavior of the consumers by sending false messages to mimic the demand response program either before, after or during a peak consumption state [154, 155]. An advantage to attackers is that there are multiple entry points to carry out a demand manipulation attack. Unlike attacks on SCADA systems, there are a variety of options that can be used to manipulate the demand—using IoT devices, energy theft and social engineering as a tool to make people perform a task. They also do not require access to the system operations or understand how the grid works. It follows a black-box approach with attackers not requiring power grid domain knowledge, thus making it an option for a variety of adversaries.

Demand manipulation attacks are the newest kinds of attacks that do not test the security of the power grid systems, but affect the power grid from the utility side by changing the demands of the consumers. There are successful DDoS attacks using IoT devices and botnets that were previously carried out (e.g. Mirai botnet attack) and there are open security issues when it comes to IoT devices and protocols. Since power grid devices and the consumers cannot be removed from the power grid scenario, but are used as a tool to perform adverse attacks, there remains an advanced persistent threat to the power grid. Though communication networks and power grid devices are being enhanced in terms of security, the threat from consumers will always exist until host-based anomaly and intrusion detection systems are established in

each home. We discuss two attack examples that were proposed by [187] and [154].

4.2.1 Attack Example 1: Demand manipulation using IoT devices

The poor security measures and ubiquity of IoT devices have been an advantage to attackers for creating botnets to perform DDoS attacks. Access to compromised high-wattage devices can allow an adversary to disrupt the power grid's normal operation by manipulating the total power demand. Since there are many types of IoT devices in a household, a common question is whether it is possible to get access to all of them. However, by gaining access to home assistants such as Amazon Echo or Google Home, control of such devices is possible [187]. The attack model is described below.

- The adversary obtains access to various high-wattage IoT devices such as air conditioners, space heaters, and electric ovens from multiple households in the same geographical location.
- If the target of the attack is the generators, then an abrupt increase or decrease in the power demands causes frequency instability of the generators resulting in their tripping. This is achieved by synchronously switching on/off many high wattage devices. A black start is a system's restarting process after a blackout, which can also be disrupted by causing frequency instability in the system.
- When a frequency instability that does not have a significant effect happens, the primary controller of the generators stabilizes the system frequency. Line failures and cascading failures can be caused by increasing the demands, as an increase of only 1% can cause an outage in 86% of the loads at this stage when simulated in the 2008 Summer peak Polish Grid. The reason these lines are sensitive is because the way power is transmitted follows Kirchhoff's laws and the grid operator has almost no control after the response of the primary controllers. Line failures can also occur by redistributing demand via increasing demand in some places and decreasing demand in others.
- An increase in the operating costs is caused when the demand goes above the predicted demand; this is when the operator needs to purchase additional electric power from reserve generators. By simulations, it is observed that a 5% increase in power demand during peak hours results in a 20% increase in power generation costs.

4.2.2 Attack Example 2: Demand manipulation using social engineering

Research in behavioral psychology predicts that people who are normally lulled into a sense of cognitive ease, do not question the validity of the information unless it is significantly different than those from previous events [154]. Based on this expectation, Raman et al. report an unconventional mode of malicious attack which demonstrates that consumer behaviors could be manipulated by an attacker using false communications that could significantly impact the system reliability [154]. The attack model is described below.

- The adversary obtains access to some form of media such as SMS, e-mail or other platforms that could be used to send legitimate communications to the residents.
- The adversary invites the consumers to participate in an upcoming Demand Response (DR) event, with the time, duration and task specified. At the same time, the attacker also needs to block communications from the utility company.
- The consumer who receives the message decides whether to accept or reject the DR event request. If the consumer accepts the event, then they take steps either manually or using an automated home energy management system (HEMS) to reduce consumption during the specified event period.
- The attack can be performed to fake a DR event or before a real DR event takes place. The resulting overshoot in demand due to the fake event would reduce the effect of the consumer response to the actual event. These messages can be sent to fake maintenance shutdown alerts, suggesting the consumers to use appliances during high stress time periods. They can also be used to follow a legitimate DR message sent by a utility to declare that an event was canceled.
- For example, the consumers might be asked to schedule washing machines, dryers and dishwashers during a specific time like 7 PM to 9 PM. Right after a peak demand time, if these high-wattage appliances are switched on, then it would impact the performance of tap changing regulators which would have to respond to the sudden change in the system voltage. Prolonged operation of such appliances can deteriorate the life of such transformers having to work under high loading conditions. It is observed in simulations that if 50% of consumers believe the fake message, the attacker could alter the system's daily peak demand by more than 2% which is quite significant to the utility.

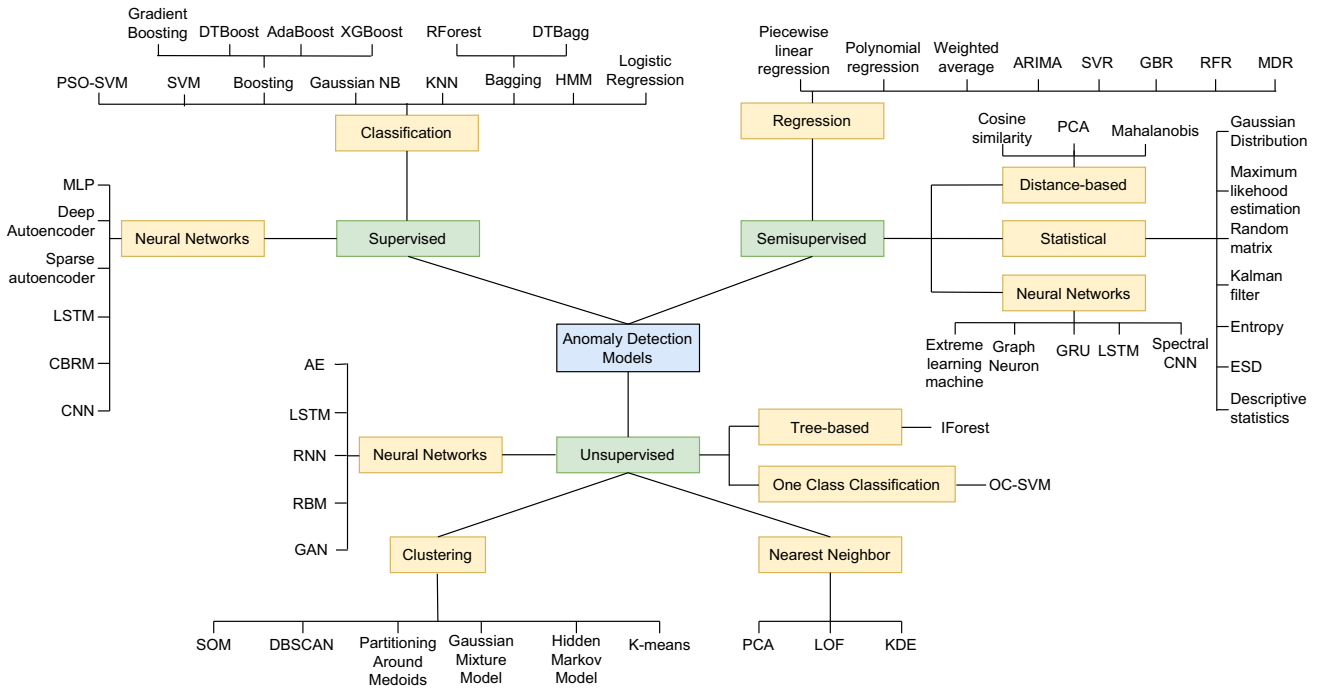

Fig. 6 Taxonomy of anomaly detection algorithms discussed in this work; Table 4 provides the list of works under a specific detection technique

4.3 Attack impact

When attacks are carried out such that the physical components are affected, then the power grid operation is hindered, due to which the consequences are likely to be catastrophic. Any attack that collapses the power grid has cascading effects on other critical infrastructure as well, like water treatment plants and food production industries. Many people will be affected by the lack of basic elements that are necessary to sustain life in urban and suburban communities.

Some believe that the cyber threat to critical infrastructure is rather exaggerated. This is because cyber threats to this infrastructure that belongs to the nation have never caused the loss of human life, never injured a person or never damaged a building [164]. However, damage to the physical equipment requires bringing in new or reserve equipment that affects the operational costs. Power outages cost between $18 and $33 billion per year in the United States. The most recent 2021 Texas power crisis which was caused due to winter storms resulted in a $20.4 billion excess expenditure, being the most costly winter event in the US affecting 10 million people and resulting in more than 150 deaths [129]. Therefore, cyber attacks combined with climate and other external factors, can lead to heavy damage and losses to the power grid.

The energy industry is far behind most other industries when it comes to security best practices and maintaining systems as these industrial systems rely on 1970 s-era technology. It doesn't get upgraded, because doing so would interrupt service [140]. The root causes of the increasing number of blackouts are aging infrastructure and a lack of investment and clear policy to modernize the grid. Also, electricity demand has grown 10 percent over the last decade, even though there are more energy-efficient products and buildings than ever [130]. Hence, the problem is only getting worse with this combination of legacy systems and increasing demands. The electric power industry spends over $1.4 billion annually to replace electromechanical systems and devices that involve manual operation with new SCADA equipment [213]. This shows that investment in physical infrastructure and security is consistent every year, but the progress is slow. This gives time for attackers to take advantage of vulnerabilities that are persistent in the power grids.

4.3.1 Physical impact

As power needs to be delivered to a large scale of consumers, it is impractical and costly to have electric power storage for them. Therefore, stable operation of the power grid relies on a balance between the power supply and demand. The demand is usually estimated by the operator based on the weather data and historical consumption data. This allows them to deploy enough generators to meet the demand beforehand, without overloading any power lines. The increase or decrease in demands, thus leading to an increase or decrease in the frequency of the system cannot be tolerated for a long time since frequencies lower than a nominal value cause severe damage to the generators. An unpredicted supply and demand setting may result in electric power overload on some of the power

lines. Once a line is overloaded, it may be tripped by the protective relay, or it may break due to overheating which should be avoided by the relay. Another issue is voltage instability caused when the generated power becomes inadequate. In such cases, power flow equations fail which forces the grid operator to perform load shedding to recover the system from the voltage collapse and make the equations feasible again. This causes outages around the grid due to failures in a few lines. Failure of components such as generators, lines or transformers has a high impact on the operation of the grid. It might result in even a blackout and when the system tries to recover from a blackout (black start), it is weak and more vulnerable to a repeated attack which can have adverse effects on the frequency of the operation.

5 Anomaly detection methods in power grid

Anomaly detection methods are broadly classified into three approaches: supervised, semisupervised and unsupervised [29]. In this summary, each of these categories is further divided into sub-categories based on the detection technique. An overview of the detection techniques discussed is shown in Fig. 6. The list of works utilizing a specific detection technique is available in Table 4.

5.1 Supervised approaches

Supervised anomaly detection is a technique that assumes the availability of labeled training data for both normal and anomalous classes. A typical approach is to build a predictive model and compare unseen data against the model to determine the class it belongs to [29]. In this subsection, we categorize supervised techniques into classification-based and neural network-based models.

5.1.1 Classification

Classification is used to learn a model (classifier) from a set of labeled data instances (training) and then, classify a test instance into one of the classes using the learned model (testing) [29]. Several traditional classifiers are known and are used in power grid applications namely, Logistic Regression (LR) [133], Gradient Boosting, Gaussian Naive Bayes (GaussianNB) [2, 37, 142], AdaBoost, XGBoost, Decision Tree (DT) [2, 68], Decision Tree as base learner (DTBoost), K-Nearest Neighbors (KNN) [72, 159], Multi-layer Perceptron classifier (MLP), Quadratic Discriminant Analysis (QDA), Support Vector Machine (SVM) [2, 42, 54, 95, 173], bagging ensemble classifier with decision trees as base learner (DTBagg) and Random Forest classifier (RForest) [2, 95, 137, 142]. The classification techniques are applied for different detection tasks like anomalous power consumption, anomalous network traffic, denial-of-service attacks on communication networks, electricity theft, false data injection, intrusion and tripping attacks.

Traditional classifiers are used by Xu et al. to determine anomalies in the running power consumption data of the Distribution Terminal Unit (DTU) as the consumption is influenced by the strong correlation to its running programs [220]. If the DTU is attacked, the running program will be modified slightly that influences the consumption as well. Two other works also compare different classifiers and different sampling techniques to solve the imbalanced data problem i.e. unequal distribution between the classes [109, 149]. Wang et al. perform a similar comparison and propose a novel model in which random forest is used as the basic classifier of AdaBoost followed by weighted voting on the prediction labels to decide the final class [203]. AdaBoost is also used by Qu et al. for detecting electricity theft attacks in residential areas using the power consumption data [152]. To provide wide area protection of the smart grid, Singh and Govindarasu evaluate different classification techniques for sensor data to detect multiple attacks like FDI, DoS, lines tripping and cyber events [181].

Classification can be performed on features that are extracted or modified for better performance of the classifier. Al-Abassi et al. pass the voltage data to a stacked autoencoder to obtain a different representation of the input data and apply random forest for classifying the anomalous data [5]. Ouyang et al. propose a hierarchical time series feature extraction algorithm and an ensemble classification model that uses XGBoost, RForest, and LR [138, 139]. The extracted time-series features are mainly used to find the abnormal sample distribution rules as well as the information from normal power consumption activities. Li et al. propose a blockchain-based anomaly detection based approach to detect anomalous consumption in smart grids using KNN [102]. They use different sensor data from the smart grid which records environmental factors and also use smart meter data to analyze the power consumption in combination with the sensor data.

Support Vector Machine (SVM) is used in several works from the literature by combining it with other methods. Zhang et al. first use an unsupervised approach, Gaussian Mixture Model Linear Discriminant Analysis (GMM-LDA) to label the consumption data and send it to Particle Swarm Optimization Support Vector Machine (PSO-SVM) for training with labeled data. Then, the test data is classified using the SVM model to identify the labels of the new data whether it is abnormal or not [236]. Another work also uses PSO and one-class SVM (OC-SVM) for the detection process [211]. Wang et al. propose an efficient home power anomaly detection using SVM and Hidden Markov Model with improved monitoring performance in terms of electricity usage as well as changes in the daily living activities of residents via

the provision of detailed feedback [209]. Wang et al. propose a supervised learning algorithm named Support Vector Machine embedded Layered Decision Tree [206]. First, it segregates the training data set into subsets based on all nominal features which reduces the dimensionality of the feature space. Then, for each subspace, only the numeric features are considered to run Decision Tree-based Support Vector Machine. SVM is applied recursively to the tree to detect the anomalies. This detection process is carried out by each agent separately, but the final decision depends on the consensus among all interconnected agents.

5.1.2 Neural network

Artificial and deep neural network models can be useful in learning patterns and generalizing from past data to identify normal and anomalous instances [73]. Feedforward and recurrent neural networks are used for prediction and classification tasks in power grid anomaly detection.

Yuan and Jia use smart meter data for detecting anomalies but is done in a distributed manner where an IoT-based distributed structure is implemented to execute the data interaction [231]. They propose a deep learning approach that uses a stacked sparse autoencoder which is a multi-layer neural network consisting of several basic sparse autoencoders followed by a softmax layer for classification. Reuter et al. use a deep feed-forward neural network for classification and a deep autoencoder for the detection of anomalous data in SCADA communication systems [163]. Wang and Ahn use time series modeling in combination with an artificial neural network, SVM and KNN to yield accurate results for the detection of anomalies in residential application [208]. The artificial neural network is used for consumption prediction and to compensate for the non-linearity that traditional time series models like ARIMA fail to capture.

Wavelet transform (WT) provides a unified framework for signal processing applications. WT can decompose a signal in coefficients, and it can localize an anomalous behavior in both the time and frequency domains with different scales. Hence, Ghanbari et al. use WT followed by variance fractal dimension (VFD) to measure the complexity of the coefficients extracted during WT [61]. Additionally, they use a feed-forward artificial neural network to enhance the detection rate of anomalous behaviors in a short duration of the attack.

Some attacks involve hijacking the controller code that controls the actuators of the physical system, making the control behave abnormally. The PLCs consist of the control code to perform a specific task in the power grid. They are relatively stable as the code running on the controller changes infrequently. The key idea for the detection used by He et al. is that the normal behavior of the controller is predictable using a temporal deep learning model and low-cost Hardware Performance Counters (HPC) features [70]. LSTM and Conditional Restricted Boltzmann Machine (CRBM) are used to predict normal controller behavior and a reconstruction error distribution of HPCs is used to detect controller anomalies. The squared error of the actual and the predicted behavior is used to indicate the anomalies. LSTM is also used for predicting power consumption data in a supervised manner by training with normal and abnormal samples [199].

Efstathopoulos et al. use operational data and examine whether smart grid attacks can be detected by analyzing them [48]. Operational data is generated from physical devices that are used to run the power plant, e.g. temperature of a cooling system. They apply and compare different techniques like PCA, Isolation Forests (Iforest), Angle-based outlier detection (ABOD), one-class SVM, Stochastic Outlier Selection (SOS) and deep fully connected autoencoders. Wilson et al. use stacked autoencoder to develop machine learning features against transmission SCADA attacks [215]. The network is first pretrained with a greedy layer-wise pre-training procedure after which the parameters of the whole deep network are initialized by the corresponding parameters learned. After the training phase, a classifier layer is added to the deep neural network model and the fine-tuning takes place in a supervised manner.

Convolutional neural networks are used for image anomaly detection by actively monitoring fire breakout and working personnel [77]. Supervised classification is also achieved by adding a classifier layer to a neural network [171]. Such a method is used in [22, 43, 234] to identify anomalies in voltage data from the distribution power lines and traffic packets in communication networks using a CNN. Moreover, [234] uses multi-headed attention before classification to capture the multi-dimensional relationship between each packet from the traffic cluster.

5.2 Semisupervised approaches

Semisupervised techniques assume that the training data has labeled instances only for the normal class. Since they do not require labels for anomaly class, they are more widely applicable. The typical approach used in such techniques is to build a model for the class corresponding to normal behavior and use the model to identify anomalies in the test data [29]. We categorize semisupervised techniques into regression-based, distance-based and statistical models.

5.2.1 Neural network

Pattern matching is the ability to store known patterns of information flow within a given network and to perform a rapid comparison of real-time information with stored correlations in sub-patterns stored previously. The correlation between localized device readings is viewed as a pattern.

As the power grid networks contain resource-constrained devices, Baig proposes an in-network, light-weight decentralized pattern recognition algorithm which can form an associative memory structure by interconnecting individual SGI device readings in a graph like structure called the GN (Graph Neuron) array [19]. The GN-based pattern recognition process is a comparison of SGI device readings at any given point in time to establish conformance with normal readings.

An extreme learning machine-based (ELM) anomaly detection technique is used in edge devices that enables on-device learning and detection [197]. LSTM and Gated Recurrent Unit (GRU) are used for predicting the power consumption and the loss between the predicted and actual is used for the anomaly detection process [58, 62, 113, 131, 143, 194, 210, 219, 242]. Spectral residual CNN is used by Oprea et al. to detect anomalous usage in residential consumption data [136].

5.2.2 Regression

The basic regression model-based anomaly detection technique consists of two steps. In the first step, a regression model is fitted to the data. In the second step, for each test instance, the residual for the test instance is used to determine the anomaly score. The residual part (e.g. anomaly score) is not explained by the regression model and can be chosen based on the use case.

Demand response programs are designed to reduce energy consumption for relatively short time periods and are widely recognized to help meet both reliability and market needs. However, it is critical to predict the reduction in energy during events and the increase due to the rebound effect after events. Zhang et al. focus on predicting the consumption accurately specifically for demand response programs [238]. A piece-wise linear regression is performed using the correlations between temperature and consumption to be able to predict the consumption accurately. An instance is then classified as an anomaly if the ratio of the predicted and observed consumption values are less than a threshold that depends on the historical consumption data of the user.

Badrinath Krishna et al. use ARIMA for power consumption prediction followed by computing time-window statistics of mean and standard deviation for detecting electricity theft [18]. Janetzko et al. use a prediction-based anomaly detection method using weighted average prediction by using daily seasonality and compute a normalized anomaly score for the detection process [87]. Higher anomaly scores denote a higher chance of it being an anomaly. Alighol-ian et al. use support vector regression (SVR) as a load prediction method, after which the difference between the real and predicted data is characterized by using a distribution function to detect the outliers with a 3-sigma rule [7]. Hosseinzadehtaher et al. propose a condition monitoring vector (CMV) equipped with a learned ultra short demand forecasting (USTDF) mechanism for detecting anomalies in AMI readings and smart inverters data [76]. The USTDF is based on the consumption data and temperatures and this model is built using multi-dimensional regression (MDR). Jaiswal et al. use four different types of regression techniques including linear regression, random forest regression (RFR), support vector regression (SVR) and gradient boosting regression (GBR) on consumption data followed by a 2-standard deviation for tagging anomalies [85].

Hybrid models are usually developed when different models perform better in different time windows. Cui et al. propose a detection system for school electricity data that combines polynomial regression for weekends and Gaussian distribution for week days [39]. Polynomial regression with Hampel identifier is used by Huang et al. for detecting anomalous consumption values in a research facility [79]. Kosek and Gehrke use an ensemble of non-linear artificial neural network models to detect anomalies in distributed energy resources (DERs) in a power grid that can be accessed and controlled remotely [97]. This model uses contextual parameters like hour of the day and other meteorological data for the training and detection process.

5.2.3 Distance-based techniques

Chen et al. use a Multi Layer Perceptron (MLP) and Mahalanobis distance-based statistical approach to find anomalies in power consumption data [30]. Yijia and Hang propose a detection method for identifying abnormal electricity users by combining the line loss and power analysis [228]. They use the Slope Extract Edge Point(SEEP) algorithm to extract the edge point sequence of power consumption and then apply the vector space cosine similarity to measure the similarity between the extracted sequence and the consumption sequence of the users. Consine similarity matching is applied after a Kalman filter estimation in [160], for detecting FDI attacks in smart grid communication systems.

Valenzuela et al. use principal component analysis (PCA) on the power flow data of the power grid transmission system and use principal components in the new subspace as well as the original values to construct an anomaly score [201].

5.2.4 Statistical models

Several works use matrix-based methods to find the changes between the states as the base for detecting anomalies in the target network [193, 237]. Zhang et al. used random matrix theory to detect anomalies in big data which can include a large volume of operational data in real-time such as power consumption, voltage, current, active power, and reactive power [237]. These data are usually random due to distur-

bances from external factors like climate or electrical factors like technical failures. Hence, a random matrix is used to denote these random variables. After constructing a high-dimensional random matrix, the sample covariance matrix is determined by approximating it using maximum likelihood estimation, subjecting it to a unitary singularization treatment and calculating its eigen values. Mean Spectral Radius (MSR) is used as the metric to represent the mean distance between all of the eigenvalues and the center on the complex plane. The single ring law is used to determine the extent of random deviation of the data in a random matrix. To detect anomalous behavior in transmission lines and buses, Moslemi et al. use covariance matrices for voltage, current and frequency data [126].

Replay attacks aim to intercept authentication information. In the smart grid, replay attacks intercept the usage pattern along the varying smart meters and replay this data to carry out an undetected intrusion. Kalman filtering along with a chi-square detector is used for the detection of the replay attack for the system controller of the smart grid [240]. Kalman filter-based technique is also used in [90, 160].

Yilmaz et al. consider a hierarchical data collection smart grid infrastructure and propose a general and scalable mitigation approach called Minimally Invasive Attack Mitigation via Detection Isolation and Localization (MIAMI-DIL) [232]. The authors use Geometric Entropy Minimization (GEM) with Cumulative sum (CUSUM) to learn the minimum volume sets that represent the nominal probability distribution of the expected data instances. If a data instance is out of this distribution, then it is an outlier. Entropy-based metrics, such as normalized entropy and Shannon entropy, can be calculated on the selected features. An attack can be identified based on the value of the calculated entropy [80, 88]. For finding anomalies in load data, extreme studentized deviate test (ESD) is used in [212].

Nasr and Varjani propose a statistical anomaly detection method that uses mean and standard deviation techniques to learn the behavior of the system over time and then use a threshold to differentiate between normal and anomalous data in SCADA systems [128]. Kwon et al. also use mean and standard deviation to detect DoS and other communication network attacks [100, 101]. Ishimaki et al. use harmonic to arithmetic mean ratio-based detector to identify false data and preserve the privacy of the consumers using fully homomorphic encryption (FHE) scheme called the Cheon-Kim-Kim-Song (CKKS) scheme [83].

Karimipour et al. use a detection method based on statistical correlation between measurements [91]. Marino et al. propose a detection system that models the communication network using Poisson distributions while using data to learn the model parameters [116]. Matthews and Leger use fano factor to tag anomalies in streaming PMU data in the distribution network [121].

5.2.5 Rule-based techniques

Rashid et al. propose a rule-based system to detect anomalies at the application level [158]. Most of the detection mechanisms focus on meter-level detection which does not identify the anomaly causing appliance. The authors use both submetered and non-intrusive load monitoring (NILM) data and perform post-processing on the NILM data to improve the performance of the detection process. Azizi et al. also use a rule-based approach to detect anomalous usage in household consumption data by using non-intrusive load monitoring [17].

A hierarchical architecture is used for monitoring the micro-phasor measurement unit data, by providing a set of rules based on different events and using correlation matrices to examine the state of the grid [86]. Zhang et al. propose a time series anomaly detection model that is applied on the network level packets in the power grid communications between SCADA's HMI and PLCs [235]. It is based on Discrete Fourier transform, and periodicity of network packets which are then checked for abnormality based on the time deviation period.

5.3 Unsupervised detection

Unsupervised anomaly detection is a technique where we do not require training data, thus making it most widely applicable. It is based on the assumption that the normal instances are frequent when compared to the anomalous ones. This assumption will prevent the technique from having a high false positive rate [29]. For building models that do not have prior knowledge about anomalous consumption, the model is trained using the normal consumption behavior along with the definition of classifying consumption values as abnormal or normal [73].

5.3.1 Clustering

Clustering is a machine learning scheme used to categorize unlabelled consumption data into various clusters, mainly normal and abnormal clusters. Clustering can also be done on normal data and the data points that are farther away from the formed normal clusters are usually tagged as anomalies [233]. Some of the common clustering methods used in the context of power grids are K-means, Partitioning Around Medoids (PAM) [14, 169, 185] and Density-based spatial clustering of applications with noise (DBSCAN) [60, 62, 137, 243],

K-means clustering is a popular unsupervised approach that is used to categorize the observations into k clusters with the nearest means or the cluster's centroid. This method has been used for detecting anomalous power consumption in residential buildings [49, 117], flooding of UDP packets,

ICMP packets and Ping of Death in communication networks [122] and anomalous behavior in a distributed framework on network and PMU data [188]. Two clustering methods are also combined to achieve better performance in detection. K-means and Isolation Forest (IForest) are used in communication networks [177] and distribution PMU networks [93]. Rahimi et al. use a genetic algorithm to get an optimal K value for the K-means to find anomalous usage in power consumption data [153]. A combination of clustering and prediction methods, specifically K-means and LSTM is used by [27, 28, 59] to cluster the consumption observations to detect the anomalies as well as find anomalies in advance by using the prediction method (i.e. LSTM) to forecast the value into the future. Chou and Telaga also followed a similar approach by using K-means followed by a combination of neural networks and autoregression (NNAR) [34].

In an attempt to detect contextual and collective anomalies, Rossi et al. propose an approach based on frequent itemset mining by encoding the different event types streamed from smart meters, applying segmentation of the data and using categorical clustering for the evaluation of the collective data and detection of unexpected patterns [165]. Contextual information is also used by [14, 169, 185] to detect anomalies in the consumption by computing an anomaly score for each user considering historical consumption data. The anomaly score for a user is then adjusted by analyzing other contextual variables such as seasonal variation day of the week and other users with the same historical pattern. All three works use models based on Partitioning Around Medoids (PAM). PAM is also used for anomaly detection in solar farms on voltage and current data that is collected from micro-PMUs [44].

Commercial buildings consume a lot of energy and hence, motivate research to improve building energy efficiency. Bellala et al. propose an anomaly detection mechanism for power meter data to detect anomalous points using an unsupervised cluster-based algorithm to model the occupancy using Hidden Markov Model [24]. This algorithm takes as input the power time series of a meter over several days and outputs the probability of a particular day being anomalous. The values are computed through a KNN density estimation algorithm. The probability scores can be used to rank the days in terms of anomalousness, providing a building administrator with a prioritized list of data points that require further inspection. Janetzko et al. use the same clustering-based approach to detect anomalies in power consumption data and provide various time series visualization schemes, which helps in analyzing and understanding the energy consumption behavior [87].

DBSCAN is used for detecting anomalous behavior in IoT devices [60], phasor data from PMUs [243], streaming consumption values [62] and communication networks [137]. Zhang et al. propose an anomaly detection method for smart meters data which is based on Gaussian Mixture Model Linear Discriminant Analysis (GMM-LDA) clustering used for feature learning [236]. Self-Organizing Maps (SOM) is an unsupervised machine learning technique used to produce a low-dimensional representation of a higher dimensional data set while preserving the topological structure of the data. SOMs are used in [200] and [196] for detecting faults and FDI attacks using consumption data.

Visual analysis makes it easier to identify anomalies on a large scale. When analyzing data streaming from multiple sensors, it is important to identify similar patterns among them, so that the sensors can be grouped based on their behavior. This grouping can be done by using similarity measures between the different streaming data [189]. This aids in the initial analysis of the sensor data coming from a power grid, that can be used for creating anomaly detection models that represent the underlying patterns. Similarly, dissimilarity measures are also used to cluster similar groups together [65].

5.3.2 Neural network

Neural networks are used in anomaly detection techniques to let the network itself discover the patterns, features from the input data and the relation of the input data over the output.

Recurrent neural networks (RNN) are used for predicting the time series. It is used by Xu et al. for power consumption data followed by quantile regression to build probabilistic power consumption forecasting models with a quantile interval that is chosen beyond which the instance will be flagged as an anomaly [222].

Autoencoders are used to reconstruct the input data with the reconstruction error as the anomaly score that gives the extent to which the reconstructed output is different from the input. The input can consist of multiple features that are contextual or behavioral (day of the year, season, month, etc.) along with power consumption [12, 13]. Other neural networks can be combined with autoencoders like a variational autoencoder combined with RNN and attention [127, 146] for power consumption data or a CNN with an autoencoder [40] for smart home sensor data. Autoencoders are also used for anomaly detection in the power generation process specifically for wind turbine fault detection [239] and inverter sensors in solar power plants [82]. They are also used for PMU data in the power grid distribution network [3].

Generative adversarial networks (GANs) consist of a generator that generates adversarial samples and a discriminator that is trained on differentiating anomalous data from normal data. This is used for detecting intrusion attacks in communication networks that can occur in any smart grid infrastructure consisting of communicating IoT devices [36, 184] as well as in a federated setting [1].

Restricted Boltzmann Machine (RBM) is used for detecting large-scale attacks in the transmission lines using the voltage and current data [92].

5.3.3 Nearest neighbor and density-based techniques

Principal component analysis (PCA) is used by [114, 151] for selecting features that represent trend, variability, volatility and other statistically representative data of the consumption. Qui et al. use the first two principal components to represent the power consumption pattern of each user [151]. Local Outlier Factor (LOF) is used to quantify the extent to which each user's point is an anomaly. LOF uses a concept of local density where each data instance needs the distance of its k nearest neighbors. Large distances result in low-density regions for anomalous data instances as compared to normal data instances. LOF is also used in communication networks for identifying anomalous traffic packets [64] and in commercial and residential buildings [156, 157]. Shylendra et al. use kernel density estimation (KDE) for detecting anomalous usage in power consumption data for wide sensor networks [178].

5.3.4 Tree-based techniques

Isolated forest is an unsupervised technique based on the decision tree algorithm. It is used for detecting anomalies in communication networks [64, 177], household power consumption [7, 114], power grid parameters in SCADA systems [175], inverter sensors in solar power plants [82] PMU data [93] and micro-PMU data in distribution networks [50].

5.3.5 One class classification

One class SVM is an unsupervised approach that uses only normal instances for the training and categorizes the data that deviate from the estimated model as anomalies. Though the performance of OC-SVM is similar to a binary class SVM, OC-SVM is preferred as it is trained only on normal data and detects anomalies from the new data by comparing it to the normal behavior [45]. It is used for identifying attacks in power consumption data of IoT devices [72, 211], communication networks [64] and transmission lines [51, 217].

5.4 Other techniques

Other techniques that have been used in smart grids include hierarchical temporal memory (HTM) [21] for anomalous behavior of micro-PMU data, an online model-free reinforcement learning approach which does not require attack models [23, 99] and an evolutionary technique based on fuzzy learning for improving clustering performance [105]. Passerini et al. use power-line communication signals to identify and localize faults in the distribution network such as electrical faults, impaired cables and unexpected impedance changes [145]. They utilize a two part algorithm, the first detects and tracks the evolution of faults over time while the second uses information about the network topology to localize the faults identified by the first algorithm.

5.4.1 Graph-based techniques

By using nodes and edges in a graph to represent the buses and branches in the electric network, graphs are constructed using the topological information of the network. The power grid is represented as a graph and the topology change is observed over a time period [104]. Anwar and Mahmood propose a graph matching approach to detect anomalies that exist in an electric topological and configuration database [11]. A query graph is anomalous if it has different number of nodes or edges than the reference graph. Graph-based techniques are also used to represent edge devices [221], sensors in smart homes [125] and transmission lines [75]. Chen et al. propose a graph technique that uses correlation grouping [31] and a graph convolution network with attention [33] to learn graph structures of the sensor data in power grids.

5.4.2 Big data

For data-driven anomaly detection, the processing of big data often becomes a challenge [204]. Lipcak et al. showcase the application of big data platforms using Apache Flink, Storm and Spark and compare the performances of the three while using weighted average prediction using previous three days of the consumption data and the temperature [106]. Apache Spark and Spark Streaming are also used for creating distributed computing framework [47, 108]. Chen et al. aim at implementing an online real-time detection algorithm for handling huge amounts of data using Storm and Hadoop-based framework [30]. For processing large-scale data from smart meters, Moghaddas and Wang propose a hierarchical framework that uses smart meter event data rather than consumption [123]. Matthews and Leger leverage MapReduce for the processing of millions of data from the PMUs and detect anomalies [120].

6 Future challenges

Our extensive review highlights that anomaly detection in the power grid is an active area of research, and continues to see novel explorations. At the same time, this broad look at the variety of work performed helped us identify recurring challenges in the domain. In this section, we discuss those pressing challenges that persist in the area despite advances in the complexity of adopted methods.

6.1 Detection speed and accuracy

For critical infrastructure like the power grid, real-time monitoring is essential and plays an important role in the grid operator's decisions. The importance of applying quick detection approaches for not missing alarms during an active attack is also addressed in the literature [38]. However, when it comes to the detection of attacks, there is always a question as to when to raise an alarm. The earlier the anomaly is detected and reported, the sooner appropriate actions to mitigate the impact could be undertaken [4]. With many threshold-based approaches used in detection systems, having too small of a threshold raises false alarms and having it too large might miss anomalous instances. The selection of a threshold plays a crucial role in anomaly detection. As such, it is important to study the trade-off between detection reliability and detection speed and to operate on the optimal trade-off curve. In [112], it is shown that as the threshold is increased for a power consumption anomaly detection system, the detection rate or the true positive rate becomes worse and on the other hand, the false alarm rate or the false positive rate improves. During this analysis, it is observed that even when obvious anomalies that have very high wattage are injected, the detection system is still unable to capture them. Though an optimal threshold is chosen, the undetected attack configurations still lead to a successful attack on the power grid. Therefore, considering the detection accuracy alone leads to an inevitable trade-off between the true positive and false positive rates which must be assessed before deploying a model.

6.2 Concept drift and evolving attacks

Detection model updates over time are inevitable given that a consumer's energy usage changes throughout the year. For example, when a new appliance is added or the number of members in the household change, the consumption pattern also is affected [238]. Therefore, handling concept drift and distribution shifts in the data is an important aspect of detection models. However, this is not commonly discussed when proposing new techniques.

Supervised detection algorithms perform better when detecting known attack signatures. Due to the unavailability of labeled data, detection becomes challenging when new attacks come to the surface. It is required to have robust mechanisms that can be updated to detect different types of evolving attacks [16]. Though a semi-supervised or unsupervised mechanism can be deployed for such a case of varying attacks, there is a possibility for an attack to be constructed such that it works within the tolerance levels of a model and stay undetected. Adversarial attacks on machine learning models have been shown for image data and time series data, and it remains as an advanced persistent threat to detection models.

Many power grid attacks begin with a compromise in the communication network. Therefore, using state-of-the-art countermeasures specifically for monitoring and detecting intrusions in the network will help in the early detection of an attack. Application of software-defined networking (SDN) to smart grids is known to enhance the SCADA system resilience [46]. SDN is a networking paradigm that provides separation between the control and data plane, allowing the controller to configure the network operations dynamically. If there is a failure of the network due to an attack, SDNs can be leveraged to dynamically establish a faster route via the internet as an emergency response. SDNs are also capable of dynamically filtering out unwanted traffic and potentially malicious traffic. This improves the efficiency, monitoring and resiliency of smart grid communication networks. Another promising countermeasure in industrial environments is the use of honeypots. In the context of smart grid networks, a honeypot simulates the normal operation of a device, such as a smart meter, to attract, deceive and analyze an attacker's behavior [134]. Several proofs-of-concept have been shown for the use of honeypots in smart grids [134, 147, 183]. The use of honeypots for privacy-preserving federated learning environments is discussed in [6]. Agame-based honeypot selection has also been proposed which characterizes the essence and objective of the defender to support the choice of the honeypot type [25]. This helps in studying evolving attacks on the devices and the underlying network.

6.3 Limited data

When using supervised approaches, there is an imbalance between normal and anomalous data which makes it difficult to capture the characteristics of anomalous data points. Imbalanced data refers to the unequal distribution of the data instances in different classes, usually having the anomalous class as the minority and the normal class as the majority. This arises because the data that is collected from the system is typically associated with normal behavior and not disturbances or attacks. In a lot of studies, it was proved that some classifiers achieved better overall performance with a sampled and balanced dataset [149]. This poses a challenge as to how well the detection technique can perform with such limited availability of anomalous data.

Unlabeled data poses a challenge for classification-based anomaly detection as there is no clear indication of a specific point is normal or anomalous. There is a significant lack of labeled data and new types of attacks may have a behavior different from the trained data [24], which is why unsupervised detection approaches are preferred over supervised. However, unsupervised approaches usually end up having high

false alarms, which might again misguide the grid operator in terms of taking the wrong countermeasures.

Transfer learning has become an effective approach as data and knowledge of older systems with richer power consumption records can be utilized [223]. Using this technique helps with the challenge of limited data, but there are other factors to be considered, such as device upgrades, changes in the consumption behavior of the consumers, new attack scenarios and threats, among others.

6.4 Datasets for benchmarking

Standard datasets that mimic the operation of the power grid in different locations, such as consumption at the utility level, or voltages and currents of the transmission lines, along with common anomalies or attacks that occur with such data will make it easier to benchmark methods for each target application. Though IEEE bus systems are used to generate synthetic data to mimic such operations, the artificial anomalies that are generated and the changes that are performed to the load still differ between research papers. Therefore, datasets that capture different anomalous events that are observed in the real power grid will help in obtaining a better validation of the constructed detection model.

6.5 Deployment and application in real world

While most of the detection mechanisms are trained and tested on smaller datasets, deploying the same model in the real world will be different. This is because the model begins to receive streaming data which it must handle, making it a real-time and online model. The efficiency of the model when deployed is not necessarily discussed in research papers. In fact, as the model must be trained using the historic data of its target deployment, it will then be validated on data that has different proportions of normal and anomalous instances. In most cases, the data is even unlabelled, making the detection performance to be heavily dependent on only the false positives. This changes the way a model perceives anomalies in the real world. To bridge the gap between development and deployment of detection mechanisms, the Digital Twin Technology can be used for rigorous testing and studying the detection performance of various attacks. A Digital Twin is a digital model of a physical system that reflects its behavior by applying platforms and two way interactions of data in real-time [84]. It provides a virtual environment to manipulate costly grid devices allowing the development of standardized models for the smart grids [15, 134].

6.6 Anomaly or attack source

An anomaly can be detected based on the observed data, however, finding the source of the anomaly is rather challenging [158]. Most of the detection systems are unable to find the attack source or the anomalous resources directly. In addition, to quantify an anomaly, it is also important to locate the anomaly especially as we are moving towards a distributed and federated learning environment. As the number of devices that are managed by a single detection algorithm increases, identifying the source of anomaly should also be considered.

6.7 Thresholding in detection systems

When we use a score-based system, threshold selection becomes an important step while deploying the model. Majority of the research papers use a fixed threshold that has been personalized for a specific scenario [108]. How and when to change the threshold based on the underlying behavior of the data then becomes an interesting problem. In fact, fixed thresholds have been shown to have a significant impact on the false positive rate of state-of-the-art neural networks designed for anomaly detection in the power grid [112], and leaves room for exploits irrespective of the choice made. Dynamic thresholding techniques for time series data have been proposed before. However, using or proposing such a technique for thresholding is less observed in the power grid domain [111]. As the power grid is evolving every day, dynamic or recent window-based thresholding techniques also play an important role in the performance of the detection system.

6.8 Scalability

Anomaly detection techniques proposed by different researchers aim to find anomalies in a specific dataset, that usually consists of a single target variable such as the power consumption, edge weights in graph-based approaches, or number of alarms in behavior-based approaches. However, numerous features are used to aid the detection process using a model to help in taking the decision of flagging an instance as an anomaly. For example, these features can be external temperature variables, sensors or devices in the power grid, or the number of personnel in an insider attack. With a higher frequency of data being collected for better monitoring of the grid, for example with 30 to 60 observations per second in the case of PMUs, the scope of applying the models to high frequency data needs to be evaluated for the methods in the literature. Most data available publicly usually contain one minute frequencies, which many papers are based on. However, the performance of the method in terms of timing may affect the detection results when tested on high frequency data. It is also observed that the frequency of data does affect the detection of short duration anomalies like sudden increase or decrease in demands [202]. This means that there will be an increase in the frequency of the data for bet-

ter detection capabilities. However, scalability is often less discussed in terms of the practicality of the detection model, especially with growing numbers of sensors and consumers in the power grid every day.

6.9 Distributed and edge computing

As the volume of sensors and devices in the power grid is increasing, the detection mechanisms are moving towards a distributed approach and have detection mechanisms run on-device. Classical machine learning-based methods are useful when choosing lightweight devices compared to deep learning-based methods [241]. However, they are not robust to noisy data and their performance may saturate for a large amount of data. This calls for simple methods that can be used for a single device while being able to handle streaming data without being susceptible to high errors.

Moreover, when we consider fog computing that involves fog nodes to collect and run the detection algorithm on the data from the underlying devices, it requires efficient algorithms that can handle such high dimensional data [232]. We also need to take the storage, computation and communication overhead into account when using a distributed architecture [31].

6.10 Visualization techniques for large scale data

When monitoring the power grid at a large scale, for example, monitoring the demand requirements from multiple consumers in an area, it becomes easier when using visualization compared to listing the anomaly scores. Though [87, 189] propose visual analytics to better visualize anomalies, it is not observed to be proposed in any other research work. Selecting and constructing specific metrics and visualizations related to anomaly detection is also a problem of interest. Choosing a combination of visualizations and aggregate metrics that can crunch down the anomaly metrics which are calculated for multiple devices will aid the monitoring personnel in quick detection and localization of the anomalies.

7 Conclusion

In the past few years, the attack surface of the power grid has increased with the advent of internet-based devices. In this work, we saw that past attacks that took place on the power grid were caused by infecting the ICS system with malware that is propagated over the network. We also discussed how the availability of IoT devices from the consumers has made it easier for the attacker to alter the load of the power grid leading to severe damage. These attacks and any faults that occur in the power grid can be identified by using anomaly detection mechanisms. In this work, we provide a systematic review of anomaly detection systems in the power grid while categorizing the collected 190 papers into different codes for each theme. We present a detailed taxonomy of methods that are categorized based on the availability of labeled data into supervised, semi-supervised and unsupervised techniques. Lastly, we describe the current challenges for the detection mechanisms highlighting the existing gaps and limitations, to promote further research efforts addressing the mentioned issues.

Author Contributions Srinidhi Madabhushi performed the collection and systematization of the literature, and wrote the main manuscript. Rinku Dewri supervised the collection and systematization process, and performed editorial modifications on the manuscript.

Research Data Policy and Data Availability Data sharing is not applicable to this article as no datasets were generated or analyzed during the study.

Declarations

Conflict of Interest No funding was received to assist with the preparation of this manuscript. The authors have no financial or proprietary interests in any material discussed in this article.

Human participants Our interpretation of data and presentation of information in this work is not influenced by any personal or financial relationship with other people or organizations. Copies of all papers reviewed in this work are obtained using the University of Denver's library subscriptions, or the public domain under a license with the "right to reuse" clause. This work does not involve human participants and/or animals.

Appendix

See Tables 3 and 4.

Table 3 Breakdown of references in literature by code

Theme	Sub-theme	Code	Count	References
Paper type	Review	`review`	5	[16, 71, 73, 115, 204]
	Survey	`survey`	8	[4, 8, 10, 56, 124, 226, 233, 241]
	Methodology	`big data`	3	[108, 120, 136]
		`feature handling`	6	[7, 50, 109, 138, 139, 181]
		`new method`	58	[3, 11, 12, 14, 17, 20, 22, 24, 28, 33, 34, 40, 54, 57, 61, 65, 72, 74–76, 80, 86, 90, 93, 96, 100, 104, 105, 113, 116, 125, 132, 136–139, 146, 149, 152, 153, 156–158, 176–178, 180, 184, 194, 196, 197, 209, 211, 228, 230, 234, 236, 237]
		`new methodology`	61	[1, 5, 13, 18, 19, 27, 30, 37, 44, 45, 49, 51, 58–60, 70, 77, 79, 83, 91, 92, 95, 97, 99, 105, 108, 114, 117, 120, 122, 126–128, 133, 145, 151, 159, 161, 163, 169, 171, 173, 175, 179, 181, 185, 193, 200, 201, 210, 212, 219, 221–223, 231, 232, 235, 239, 240, 243]
		`visual analysis`	2	[87, 189]
	Framework	`framework`	8	[36, 47, 102, 106, 123, 165, 188, 229]
		`architecture`	4	[88, 121, 195, 206]
	Evaluation	`evaluation`	23	[2, 7, 39, 48, 52, 62–64, 68, 82, 85, 118, 131, 142, 149, 150, 167, 191, 192, 217, 220, 227, 238]
Focus area	Targeted detection	`contextual`	7	[12, 13, 62, 96, 169, 185, 210]
		`detection`	124	[2, 5, 7, 8, 11, 14, 17–19, 21, 22, 24, 27, 28, 30, 33, 34, 37, 39, 40, 42–44, 48, 50–52, 54, 57, 58, 60, 61, 64, 65, 70–74, 76, 77, 80, 82, 87–93, 95, 97, 99, 101, 104, 105, 109, 113–115, 118, 121, 122, 125, 127, 128, 131–133, 138, 139, 142, 143, 145, 146, 149–153, 156–158, 161–163, 165, 171, 174, 175, 177, 178, 180, 184, 189, 192–196, 200, 201, 204, 206, 209, 212, 217, 219, 220, 222, 228, 229, 232, 233, 235–243]
		`drift`	2	[3, 59]
		`early detection`	2	[176, 227]
		`efficiency`	2	[79, 167]
		`optimization`	1	[211]
		`transfer learning`	1	[223]
	Big Data	`cloud computing`	1	[56]
		`data-driven`	3	[116, 166, 191]
		`distributed computing`	10	[34, 47, 106, 108, 120, 123, 126, 136, 188, 231]
		`edge detection`	3	[197, 199, 221]
		`federated learning`	4	[1, 36, 81, 179]
		`fog computing`	3	[1, 49, 85]

Table 3 continued

Theme	Sub-theme	Code	Count	References
	Profiling	behavior analysis	5	[45, 86, 100, 101, 117]
	Privacy	privacy-preserving	6	[1, 23, 36, 83, 103, 225]
	Wide Area Protection	wide sensor network	6	[137, 159, 173, 181, 182, 230]
		sensor placement	1	[75]
	Blockchain	blockchain	3	[23, 36, 102]
Data type	Single feature	consumption	84	[7, 12–14, 17, 18, 23, 24, 27, 28, 30, 34, 37, 39, 42, 45, 49, 56, 58, 59, 61, 62, 65, 71–73, 76, 79, 81, 83, 85, 87, 95, 97, 102, 106, 108, 113, 114, 117, 123, 125, 127, 131, 136, 138, 139, 143, 146, 151–153, 156–158, 165, 169, 174, 178, 185, 189, 192, 194, 196, 197, 199–201, 208–212, 219–223, 228, 229, 231, 232, 236, 238]
		current	5	[44, 75, 92, 126, 141]
		frequency	2	[126, 141]
		network	24	[2, 36, 64, 74, 80, 88, 89, 100, 101, 105, 116, 122, 137, 149, 162, 163, 171, 177, 184, 186, 188, 234, 235, 239, 240]
		sensors	15	[1, 11, 31, 33, 40, 60, 74, 82, 102, 104, 159, 161, 181, 216, 230]
		voltage	15	[5, 43, 44, 51, 58, 75, 91, 92, 96, 126, 141, 145, 168, 206, 242]
	Multiple Features	operational	24	[3, 21, 22, 44, 47, 48, 50, 68, 70, 86, 93, 99, 109, 120, 121, 128, 133, 150, 166, 175, 180, 188, 237, 243]
		system logs	2	[74, 173]
		weather	1	[210]
	Visual	image	2	[77, 241]
Grid process	Generation	generator	2	[91, 141]
		power plant	1	[48]
		solar plant	2	[44, 82]
		wind turbine	1	[239]
	Transmission	substation	6	[74, 101, 128, 193, 219, 234]
		transmission buses	2	[91, 126]
		transmission lines	7	[11, 51, 91, 92, 126, 180, 201]
		transmission sensors	3	[75, 86, 176]
	Distribution	DERs	2	[96, 97]
		distribution lines	5	[5, 43, 99, 161, 242]
		distribution sensors	17	[3, 21, 22, 47, 50, 68, 70, 90, 93, 109, 120, 121, 133, 159, 168, 188, 243]
		power line modems	1	[145]
		substation	3	[200, 217, 220]

Table 3 continued

Theme	Sub-theme	Code	Count	References
	Utility	AMI	4	[76, 95, 153, 169]
		building	9	[12, 13, 31, 34, 72, 106, 156, 157, 174]
		commercial	5	[14, 39, 79, 81, 87]
		edge devices	9	[1, 23, 60, 158, 171, 179, 197, 199, 221]
		industrial	7	[30, 65, 138, 139, 194, 223, 237]
		residential	27	[14, 17, 18, 27, 28, 58, 59, 61, 62, 85, 113, 114, 117, 131, 136, 143, 151, 152, 185, 192, 208–211, 222, 228, 238]
		smart home	4	[40, 45, 122, 125]
		smart meter	15	[7, 19, 49, 56, 57, 83, 102, 108, 123, 146, 165, 196, 229, 232, 236]
	Other	control software	2	[127, 173]
		grid sensors	21	[16, 33, 36, 42, 77, 80, 100, 104, 105, 137, 149, 177, 178, 181, 184, 204, 206, 230, 233, 240, 241]
		scada	11	[64, 88, 89, 116, 128, 162, 163, 166, 175, 176, 235]
Attack type	Attack	brute force	1	[45]
		coordinated	1	[181]
		DDoS	3	[45, 74, 232]
		DoS	9	[2, 80, 88, 100, 101, 122, 171, 177, 181]
		insider	1	[128]
		operational	1	[30]
		network	12	[2, 64, 80, 89, 105, 116, 163, 171, 184, 188, 234, 240]
		intrusion	6	[36, 74, 97, 137, 193, 201]
		FDI	17	[5, 22, 31, 54, 90–92, 99, 132, 141, 142, 159, 166, 168, 181, 196, 225]
		tripping lines	3	[142, 180, 181]
		trojan	1	[219]
		electricity theft	7	[18, 57, 118, 152, 192, 210, 229]
		demand manipulation	2	[76, 95]
		zero day	1	[70]
	Other Anomalies	fault detection	6	[51, 181, 200, 229, 237, 239]
		anomalous behavior	34	[3, 11, 19, 21, 33, 40, 43, 44, 50, 60, 68, 82, 83, 93, 104, 109, 117, 120, 121, 126, 133, 145, 149, 161, 173, 175, 188, 206, 216, 230, 235, 241]
		anomalous usage	51	[7, 12–14, 17, 24, 27, 28, 34, 39, 47, 59, 61, 62, 72, 79, 81, 85, 87, 96, 106, 108, 113, 114, 127, 131, 136, 143, 146, 151, 153, 156–158, 169, 178, 185, 189, 194, 197, 199, 209, 211, 221–223, 228, 231, 236, 238, 242]
		monitoring	4	[31, 77, 86, 220]

Table 3 continued

Theme	Sub-theme	Code	Count	References
Detection	Supervised	`classification`	22	[2, 42, 48, 54, 68, 72, 95, 102, 133, 137–139, 142, 152, 159, 173, 203, 206, 208, 209, 211, 236]
		`neural network`	17	[2, 5, 22, 34, 40, 43, 48, 61, 70, 77, 163, 171, 199, 208, 215, 231, 234]
	Semisupervised	`distance-based`	4	[30, 160, 201, 228]
		`neural network`	12	[19, 58, 62, 113, 131, 136, 143, 194, 197, 210, 219, 242]
		`regression`	8	[7, 18, 39, 76, 79, 85, 87, 238]
		`rule-based`	4	[17, 86, 158, 235]
		`statistical`	20	[39, 65, 80, 83, 88, 90, 91, 100, 101, 116, 121, 126, 128, 160, 189, 193, 212, 232, 237, 240]
	Unsupervised	`clustering`	32	[7, 14, 24, 27, 28, 34, 44, 48–50, 59, 60, 62, 64, 82, 87, 93, 114, 117, 122, 137, 153, 165, 169, 175, 177, 185, 188, 196, 200, 236, 243]
		`nearest neighbor`	7	[48, 64, 114, 151, 156, 157, 178]
		`neural network`	15	[1, 3, 12, 13, 27, 28, 36, 40, 59, 92, 127, 146, 184, 222, 239]
		`OC classification`	6	[45, 51, 64, 72, 211, 217]
		`tree-based`	9	[7, 48, 50, 64, 82, 93, 114, 175, 177]
	Other Techniques	`fuzzy learning`	1	[105]
		`reinforcement learning`	2	[23, 99]
		`graph-based`	8	[11, 31, 33, 75, 104, 125, 221, 230]

Table 4 Breakdown of references in literature by detection technique

Detection	Type	Technique	References
Supervised	Classification	Bagging	[2, 95, 137, 142, 206]
		Boosting	[2, 68, 138, 139, 152, 203]
		Gaussian NB	[2, 37, 142]
		Hidden Markov Model	[209]
		KNN	[72, 102, 159, 208]
		Logistic Regression	[133, 138, 139]
		PSO-SVM	[211, 236]
		SVM	[2, 42, 48, 54, 95, 173, 206, 208, 209]
	Neural Network	CBRM	[70]
		CNN	[22, 40, 43, 77, 171, 234]
		Deep AE	[5, 48, 163, 215]
		LSTM	[70, 199]
		MLP	[2, 34, 61, 163, 208]
		Sparse AE	[231]

Table 4 continued

Detection	Type	Technique	References
Semisupervised	Distance-based	Cosine Similarity	[160, 228]
		Mahalanobis	[30]
		PCA	[201]
	Neural Network	ELM	[197]
		GRU	[58, 194, 242]
		Graph neuron	[19]
		LSTM	[58, 62, 113, 131, 143, 210, 219]
		Spectral CNN	[136]
	Regression	ARIMA	[18]
		GBR	[85]
		MDR	[76]
		Piecewise linear regression	[238]
		Polynomial regression	[39, 79]
		RFR	[85]
		SVR	[7]
		Weighted average	[87]
	Rule-based	–	[17, 86, 158, 235]
	Statistical	Descriptive statistics	[65, 83, 91, 100, 101, 116, 121, 128, 189]
		Entropy	[80, 88, 232]
		ESD	[212]
		Gaussian distribution	[39]
		Kalman filter	[90, 160, 240]
		MLE	[237]
		Random matrix	[126, 193, 237]
Unsupervised	Clustering	DBSCAN	[60, 60, 62, 62, 137, 137, 243, 243]
		GMM	[236]
		HMM	[24, 87]
		K-means	[27, 28, 34, 49, 59, 93, 117, 122, 153, 177, 188]
		PAM	[14, 44, 165, 169, 185]
		SOM	[196, 200]
	Nearest Neighbor	KDE	[178]
		LOF	[64, 156, 157]
		PCA	[48, 114, 151]
	Neural Network	AE	[3, 12, 13, 40, 127, 146, 239]
		GAN	[1, 36, 184]
		LSTM	[27, 28, 59]
		RBM	[92]
		RNN	[127, 146, 222]
	One Class Classification	OC-SVM	[45, 51, 64, 72, 211, 217]
	Tree-based	iForest	[7, 48, 50, 64, 82, 93, 114, 175, 177]
Other Techniques	Fuzzy Learning	–	[105]
	Reinforcement Learning	–	[23, 99]
	Graph-based	–	[11, 31, 33, 75, 104, 125, 221, 230]

References

1. Abdel-Basset, M., Moustafa, N., Hawash, H.: Privacy-preserved generative network for trustworthy anomaly detection in smart grids: a federated semi-supervised approach. IEEE Trans. Ind. Inf. **19**(1), 995–1005 (2022)
2. Abdelkhalek, M., Ravikumar, G., Govindarasu, M.: ML-based anomaly detection system for der communication in smart grid. In: 2022 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference (ISGT), IEEE, pp. 1–5 (2022)
3. Ahmed, A., Sajan, K.S., Srivastava, A., Wu, Y.: Anomaly detection, localization and classification using drifting synchrophasor data streams. IEEE Trans. Smart Grid **12**(4), 3570–3580 (2021)
4. Ahmed, C.M., MR, G.R., Mathur, A.P.: Challenges in machine learning based approaches for real-time anomaly detection in industrial control systems. In: 2020 6th ACM on Cyber-physical System Security Workshop, pp. 23–29 (2020)
5. Al-Abassi, A., Sakhnini, J., Karimipour, H.: Unsupervised stacked autoencoders for anomaly detection on smart cyber-physical grids. In: 2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC), IEEE, pp. 3123–3129 (2020)
6. Albaseer, A., Abdallah, M.: Privacy-preserving honeypot-based detector in smart grid networks: A new design for quality-assurance and fair incentives federated learning framework. In: 2023 IEEE 20th Consumer Communications and Networking Conference (CCNC), IEEE, pp. 722–727 (2023)
7. Aligholian, A., Farajollahi, M., Mohsenian-Rad, H.: Unsupervised learning for online abnormality detection in smart meter data. In: 2019 Power and Energy Society General Meeting (PESGM), IEEE, pp. 1–5 (2019)
8. Alkuwari, A.N., Al-Kuwari, S., Qaraqe, M.: Anomaly detection in smart grids: a survey from cybersecurity perspective. In: 2022 3rd International Conference on Smart Grid and Renewable Energy (SGRE), IEEE, pp. 1–7 (2022)
9. Allnutt, J., Anand, D., Arnold, D., Goldstein, A., Li-Baboud, Y.S., Martin, A., Nguyen, C., Noseworthy, R., Subramaniam, R., Weiss, M.: Timing challenges in the smart grid. NIST Spec. Publ. **1500**, 08 (2017)
10. Anwar, A., Mahmood, A.N.: Cyber security of smart grid infrastructure. arXiv preprint arXiv:1401.3936 (2014)
11. Anwar, A., Mahmood, A.N.: Anomaly detection in electric network database of smart grid: graph matching approach. Electr. Power Syst. Res. **133**, 51–62 (2016)
12. Araya, D.B., Grolinger, K., ElYamany, H.F., Capretz, M.A., Bitsuamlak, G.: Collective contextual anomaly detection framework for smart buildings. In: 2016 International Joint Conference on Neural Networks (IJCNN), IEEE, pp. 511–518 (2016)
13. Araya, D.B., Grolinger, K., ElYamany, H.F., Capretz, M.A., Bitsuamlak, G.: An ensemble learning framework for anomaly detection in building energy consumption. Energy Build. **144**, 191–206 (2017)
14. Arjunan, P., Khadilkar, H.D., Ganu, T., Charbiwala, Z.M., Singh, A., Singh, P.: Multi-user energy consumption monitoring and anomaly detection with partial context information. In: 2015 2nd ACM International Conference on Embedded Systems for Energy-efficient Built Environments, pp. 35–44 (2015)
15. Atalay, M., Angin, P.: A digital twins approach to smart grid security testing and standardization. In: 2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT, IEEE, pp. 435–440 (2020)
16. Azad, S., Sabrina, F., Wasimi, S.: Transformation of smart grid using machine learning. In: 2019 29th Australasian Universities Power Engineering Conference (AUPEC), IEEE, pp. 1–6 (2019)
17. Azizi, E., Beheshti, M.T., Bolouki, S.: Appliance-level anomaly detection in nonintrusive load monitoring via power consumption-based feature analysis. IEEE Trans. Consum. Electron. **67**(4), 363–371 (2021)
18. Badrinath Krishna, V., Iyer, R.K., Sanders, W.H.: ARIMA-based modeling and validation of consumption readings in power grids. In: 2015 International Conference on Critical Information Infrastructures Security, Springer, pp. 199–210 (2015)
19. Baig, Z.A.: On the use of pattern matching for rapid anomaly detection in smart grid infrastructures. In: 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm), IEEE, pp. 214–219 (2011)
20. Barua, A., Muthirayan, D., Khargonekar, P.P., Al Faruque, M.A.: Hierarchical temporal memory based machine learning for real-time, unsupervised anomaly detection in smart grid: WiP abstract. In: 2020 ACM/IEEE 11th International Conference on Cyber-Physical Systems (ICCPS), IEEE, pp. 188–189 (2020)
21. 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 Secure Comput. **19**(3), 1770–1782 (2020)
22. Basumallik, S., Ma, R., Eftekharnejad, S.: Packet-data anomaly detection in PMU-based state estimator using convolutional neural network. Int. J. Electr. Power Energy Syst. **107**, 690–702 (2019)
23. Belhadi, A., Djenouri, Y., Srivastava, G., Jolfaei, A., Lin, J.C.W.: Privacy reinforcement learning for faults detection in the smart grid. Ad Hoc Netw. **119**, 102,541 (2021)
24. Bellala, G., Marwah, M., Arlitt, M., Lyon, G., Bash, C.E.: Towards an understanding of campus-scale power consumption. In: 2011 3rd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Buildings, pp. 73–78 (2011)
25. Boumkheld, N., Panda, S., Rass, S., Panaousis, E.: Honeypot type selection games for smart grid networks. In: Decision and Game Theory for Security: 10th International Conference, GameSec 2019, Stockholm, Sweden, October 30–November 1, 2019, Proceedings 10, Springer, pp. 85–96 (2019)
26. Case, D.U.: Analysis of the cyber attack on the ukrainian power grid. Electricity Information Sharing and Analysis Center (E-ISAC) 388 (2016)
27. Chahla, C., Snoussi, H., Merghem, L., Esseghir, M.: A novel approach for anomaly detection in power consumption data. In: 2019 8th International Conference on Pattern Recognition Applications and Method (ICPRAM), pp. 483–490 (2019)
28. Chahla, C., Snoussi, H., Merghem, L., Esseghir, M.: A deep learning approach for anomaly detection and prediction in power consumption data. Energ. Effic. **13**(8), 1633–1651 (2020)
29. Chandola, V., Banerjee, A., Kumar, V.: Anomaly detection: a survey. ACM Comput. Surv. **41**(3), 15:1-15:58 (2009)
30. Chen, H., Fei, X., Wang, S., Lu, X., Jin, G., Li, W., Wu, X.: Energy consumption data based machine anomaly detection. In: 2014 2nd International Conference on Advanced Cloud and Big Data, IEEE, pp. 136–142 (2014)
31. Chen, P.Y., Yang, S., McCann, J.A.: Distributed real-time anomaly detection in networked industrial sensing systems. IEEE Trans. Ind. Electron. **62**(6), 3832–3842 (2014)
32. Chen, T.M.: Stuxnet, the real start of cyber warfare? IEEE Network, Editor's Note (2011)
33. Chen, Z., Chen, D., Zhang, X., Yuan, Z., Cheng, X.: Learning graph structures with transformer for multivariate time series anomaly detection in IoT. IEEE Internet Things J. **9**(12), 9179–9189 (2021)
34. Chou, J.S., Telaga, A.S.: Real-time detection of anomalous power consumption. Renew. Sustain. Energy Rev. **33**, 400–411 (2014)
35. Cobb, P.: German steel mill meltdown: rising stakes in the internet of things. (2015) https://securityintelligence.com/german-

steel-mill-meltdown-rising-stakes-in-the-internet-of-things/. Accessed 01 March 2023
36. Cui, L., Qu, Y., Xie, G., Zeng, D., Li, R., Shen, S., Yu, S.: Security and privacy-enhanced federated learning for anomaly detection in iot infrastructures. IEEE Trans. Ind. Inf. **18**(5), 3492–3500 (2021)
37. Cui, M., Wang, J., Yue, M.: Machine learning-based anomaly detection for load forecasting under cyberattacks. IEEE Trans. Smart Grid **10**(5), 5724–5734 (2019)
38. Cui, S., Han, Z., Kar, S., Kim, T.T., Poor, H.V., Tajer, A.: Coordinated data-injection attack and detection in the smart grid: a detailed look at enriching detection solutions. IEEE Signal Process. Mag. **29**(5), 106–115 (2012)
39. Cui, W., Wang, H.: A new anomaly detection system for school electricity consumption data. Information **8**(4), 151 (2017)
40. Cultice, T., Ionel, D., Thapliyal, H.: Smart home sensor anomaly detection using convolutional autoencoder neural network. In: 2020 IEEE International Symposium on Smart Electronic Systems (iSES)(Formerly iNiS), IEEE, pp. 67–70 (2020)
41. Dabrowski, A., Ullrich, J., Weippl, E.R.: Grid shock: Coordinated load-changing attacks on power grids: The non-smart power grid is vulnerable to cyber attacks as well. In: 2017 33rd Annual Computer Security Applications Conference (ACSAC), pp. 303–314 (2017)
42. Dai, H., Sun, X., Li, J., Zhang, G., Ji, X., Xu, W.: Power consumption-based anomaly detection for relay protection. In: 2020 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), IEEE, pp. 1139–1143 (2020)
43. Danilczyk, W., Sun, Y.L., He, H.: Smart grid anomaly detection using a deep learning digital twin. In: 2020 52nd North American Power Symposium (NAPS), IEEE, pp. 1–6 (2021)
44. Dey, M., Rana, S.P., Simmons, C.V., Dudley, S.: Solar farm voltage anomaly detection using high-resolution μPMU data-driven unsupervised machine learning. Appl. Energy **303**, 117656 (2021)
45. Dilraj, M., Nimmy, K., Sankaran, S.: Towards behavioral profiling based anomaly detection for smart homes. In: 2019 IEEE Region 10 Conference (TENCON), IEEE, pp. 1258–1263 (2019)
46. Dong, X., Lin, H., Tan, R., Iyer, R.K., Kalbarczyk, Z.: Software-defined networking for smart grid resilience: Opportunities and challenges. In: Proceedings of the 1st ACM Workshop on Cyber-physical System Security, pp. 61–68 (2015)
47. Drakontaidis, S., Stanchi, M., Glazer, G., Hussey, J., Leger, A.S., Matthews, S.J.: Towards energy-proportional anomaly detection in the smart grid. In: 2018 High Performance Extreme Computing Conference (HPEC), IEEE, pp. 1–7 (2018)
48. Efstathopoulos, G., Grammatikis, P.R., Sarigiannidis, P., Argyriou, V., Sarigiannidis, A., Stamatakis, K., Angelopoulos, M.K., Athanasopoulos, S.K.: Operational data based intrusion detection system for smart grid. In: 2019 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), IEEE, pp. 1–6 (2019)
49. El-Awadi, R., Fernández-Vilas, A., Redondo, R.P.D.: Fog computing solution for distributed anomaly detection in smart grids. In: 2019 International Conference on Wireless and Mobile Computing, pp. 348–353. Networking and Communications (WiMob), IEEE (2019)
50. El Chamie, M., Lore, K.G., Shila, D.M., Surana, A.: Physics-based features for anomaly detection in power grids with micropmus. In: 2018 International Conference on Communications (ICC), IEEE, pp. 1–7 (2018)
51. Elmasry, W., Wadi, M.: Detection of faults in electrical power grids using an enhanced anomaly-based method. Arab. J. Sci. Eng. **47**, 14,899-14,914 (2022)
52. Elmrabit, N., Zhou, F., Li, F., Zhou, H.: Evaluation of machine learning algorithms for anomaly detection. In: 2020 International Conference on Cyber Security and Protection of Digital Services, IEEE, pp. 1–8 (2020)
53. Enerdynamics. What is a phasor measurement unit and how does it make the grid more reliable? (2021) https://www.enerdynamics.com/Energy-Currents_Blog/What-Is-a-Phasor-Measurement-Unit-and-How-Does-it-Make-the-Grid-More-Reliable.aspx. Accessed 01 March 2023
54. Esmalifalak, M., Liu, L., Nguyen, N., Zheng, R., Han, Z.: Detecting stealthy false data injection using machine learning in smart grid. IEEE Syst. J. **11**(3), 1644–1652 (2014)
55. Falliere, N., Murchu, L.O., Chien, E.: W32.stuxnet dossier, version 1.4. Symantec Security Response (2011)
56. Feng, L., Xu, S., Zhang, L., Wu, J., Zhang, J., Chu, C., Wang, Z., Shi H: Anomaly detection for electricity consumption in cloud computing: Framework, methods, applications, and challenges. EURASIP J. Wirel. Commun. Netw. **1**, 1–12 (2020a)
57. Feng, Z., Huang, J., Tang, W.H., Shahidehpour, M.: Data mining for abnormal power consumption pattern detection based on local matrix reconstruction. Int. J. Electr. Power Energy Syst. **123**, 106315 (2020b)
58. Fengming, Z., Shufang, L., Zhimin, G., Bo, W., Shiming, T., Mingming, P.: Anomaly detection in smart grid based on encoder-decoder framework with recurrent neural network. J. China Univ. Posts Telecommun. **24**(6), 67–73 (2017)
59. Fenza, G., Gallo, M., Loia, V.: Drift-aware methodology for anomaly detection in smart grid. IEEE Access **7**, 9645–9657 (2019)
60. Garg, S., Kaur, K., Batra, S., Kaddoum, G., Kumar, N., Boukerche, A.: A multi-stage anomaly detection scheme for augmenting the security in IoT-enabled applications. Future Gener. Comput. Syst. **104**, 105–118 (2020)
61. Ghanbari, M., Kinsner, W., Ferens, K.: Anomaly detection in a smart grid using wavelet transform, variance fractal dimension and an artificial neural network. In: 2016 Electrical Power and Energy Conference (EPEC), IEEE, pp. 1–6 (2016)
62. Ghanim, J., Issa, M., Awad, M.: An asymmetric loss with anomaly detection LSTM framework for power consumption prediction. In: 2022 21st Mediterranean Electrotechnical Conference (MELECON), IEEE, pp. 819–824 (2022)
63. Gholami, A., Srivastava, A.K.: Comparative analysis of ml techniques for data-driven anomaly detection, classification and localization in distribution system. In: 2020 52nd North American Power Symposium (NAPS), IEEE, pp. 1–6 (2021)
64. Grammatikis, P.R., Sarigiannidis, P., Sarigiannidis, A., Margounakis, D., Tsiakalos, A., Efstathopoulos, G.: An anomaly detection mechanism for IEC 60870-5-104. In: 2020 9th International Conference on Modern Circuits and Systems Technologies (MOCAST), IEEE, pp. 1–4 (2020)
65. Graß, A., Beecks, C., Soto, J.A.C.: Unsupervised anomaly detection in production lines. In: Machine Learning for Cyber Physical Systems, Springer, pp. 18–25 (2019)
66. Group CCESGC. Smart grid reference architecture (2012)
67. Gunduz, M.Z., Das, R.: Cyber-security on smart grid: threats and potential solutions. Comput. Netw. **169**(107), 094 (2020)
68. Hannon, C., Deka, D., Jin, D., Vuffray, M., Lokhov, A.Y.: Real-time anomaly detection and classification in streaming PMU data. In: 2021 Madrid PowerTech, IEEE, pp. 1–6 (2021)
69. Haque, N.I., Shahriar, M.H., Dastgir, M.G., Debnath, A., Parvez, I., Sarwat, A., Rahman, M.A.: Machine learning in generation, detection, and mitigation of cyberattacks in smart grid: a survey. (2020) arXiv preprint arXiv:2010.00661
70. He, Z., Raghavan, A., Hu, G., Chai, S., Lee, R.: Power-grid controller anomaly detection with enhanced temporal deep learning. In: 2019 18th IEEE International Conference On Trust, Security And Privacy in Computing And Communications/13th IEEE

International Conference On Big Data Science and Engineering (TrustCom/BigDataSE), IEEE, pp. 160–167 (2019)
71. Himeur, Y., Ghanem, K., Alsalemi, A., Bensaali, F., Amira, A.: Anomaly detection of energy consumption in buildings: a review, current trends and new perspectives. Appl. Energy **287**(116), 601 (2020)
72. Himeur, Y., Alsalemi, A., Bensaali, F., Amira, A.: Smart power consumption abnormality detection in buildings using micromoments and improved K-nearest neighbors. Int. J. Intell. Syst. **36**(6), 2865–2894 (2021)
73. Himeur, Y., Ghanem, K., Alsalemi, A., Bensaali, F., Amira, A.: Artificial intelligence based anomaly detection of energy consumption in buildings: a review, current trends and new perspectives. Appl. Energy **287**, 116,601 (2021)
74. Hong, J., Liu, C.C., Govindarasu, M.: Integrated anomaly detection for cyber security of the substations. IEEE Trans. Smart Grid **5**(4), 1643–1653 (2014)
75. Hooi, B., Eswaran, D., Song, H.A., Pandey, A., Jereminov, M., Pileggi, L., Faloutsos, C.: Gridwatch: sensor placement and anomaly detection in the electrical grid. In: 2018 Joint European Conference on Machine Learning and Knowledge Discovery in Databases, Springer, pp. 71–86 (2018)
76. Hosseinzadehtaher, M., Khan, A., Shadmand, M.B., Abu-Rub, H.: Anomaly detection in distribution power system based on a condition monitoring vector and ultra-short demand forecasting. In: 2020 CyberPELS (CyberPELS), IEEE, pp. 1–6 (2020)
77. Hou, R., Pan, M., Zhao, Y., Yang, Y.: Image anomaly detection for IoT equipment based on deep learning. J. Vis. Commun. Image Represent. **64**, 102,599 (2019)
78. Hu, Y., Yang, A., Li, H., Sun, Y., Sun, L.: A survey of intrusion detection on industrial control systems. Int. J. Distrib. Sens. Netw. **14**(8), 1550147718794,615 (2018)
79. Huang, C.C., Tsao, Y.T., Hsu, J.Y.J: Abnormality detection by model-based estimation of power consumption. In: 2012 5th International Conference on Service-Oriented Computing and Applications (SOCA), IEEE, pp. 1–6 (2012)
80. Huo, X., Lv, C., Pei, P., Gao, M., Wang, L.: Smart grid communication network traffic anomaly detection based on entropy analysis. In: 2016 2nd International Conference on Computer and Communications (ICCC), IEEE, pp. 1082–1086 (2016)
81. Huong, T.T., Bac, T.P., Long, D.M., Luong, T.D., Dan, N.M., Thang, B.D., Tran, K.P.: Detecting cyberattacks using anomaly detection in industrial control systems: A federated learning approach. Comput. Ind. **132**(103), 509 (2021)
82. Ibrahim, M., Alsheikh, A., Awaysheh, F.M., Alshehri, M.D.: Machine learning schemes for anomaly detection in solar power plants. Energies **15**(3), 1082 (2022)
83. Ishimaki, Y., Bhattacharjee, S., Yamana, H., Das, S.K.: Towards privacy-preserving anomaly-based attack detection against data falsification in smart grid. In: 2020 International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), IEEE, pp. 1–6 (2020)
84. Jafari, M., Kavousi-Fard, A., Chen, T., Karimi, M.: A review on digital twin technology in smart grid, transportation system and smart city: challenges and future. IEEE Access (2023)
85. Jaiswal, R., Chakravorty, A., Rong, C.: Distributed fog computing architecture for real-time anomaly detection in smart meter data. In: 2020 6th International Conference on Big Data Computing Service and Applications (BigDataService), IEEE, pp. 1–8 (2020)
86. Jamei, M., Scaglione, A., Roberts, C., Stewart, E., Peisert, S., McParland, C., McEachern, A.: Anomaly detection using optimally placed μPMU sensors in distribution grids. IEEE Trans. Power Syst. **33**(4), 3611–3623 (2017)
87. Janetzko, H., Stoffel, F., Mittelstädt, S., Keim, D.A.: Anomaly detection for visual analytics of power consumption data. Comput. Graph. **38**, 27–37 (2014)
88. Jung, O., Smith, P., Magin, J., Reuter, L.: Anomaly detection in smart grids based on software defined networks. In: 2019 8th International Conference on Smart Cities and Green ICT Systems (SMARTGREENS), pp. 157–164 (2019)
89. Kabir-Querrec, M., Mocanu, S., Bellemain, P., Thiriet, J.M., Savary, E.: Corrupted goose detectors: anomaly detection in power utility real-time ethernet communications. GreHack **2015**, 1–9 (2015)
90. Karimipour, H., Leung, H.: Relaxation-based anomaly detection in cyber-physical systems using ensemble Kalman filter. IET Cyber-Phys. Syst.: Theory Appl. **5**(1), 49–58 (2020)
91. Karimipour, H., Dehghantanha, A., Parizi, R.M., Choo, K.K.R., Leung, H.: A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. IEEE Access **7**, 80,778-80,788 (2019)
92. Karimipour, H., Geris, S., Dehghantanha, A., Leung, H.: Intelligent anomaly detection for large-scale smart grids. In: 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), IEEE, pp. 1–4 (2019)
93. Khaledian, E., Pandey, S., Kundu, P., Srivastava, A.K.: Real-time synchrophasor data anomaly detection and classification using isolation forest, k means, and loop. IEEE Trans. Smart Grid **12**(3), 2378–2388 (2020)
94. Kim, Y., Hakak, S., Ghorbani, A.: Smart grid security: attacks and defence techniques. IET Smart Grid (2022)
95. Korba, A.A., Tamani, N., Ghamri-Doudane, Y.: Anomaly-based framework for detecting power overloading cyberattacks in smart grid AMI. Comput. Secur. **96**, 101,896 (2020)
96. Kosek, A.M.: Contextual anomaly detection for cyber-physical security in smart grids based on an artificial neural network model. In: 2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG), IEEE, pp. 1–6 (2016)
97. Kosek, A.M., Gehrke, O.: Ensemble regression model-based anomaly detection for cyber-physical intrusion detection in smart grids. In: 2016 Electrical Power and Energy Conference (EPEC), IEEE, pp. 1–7 (2016)
98. Kumar, P., Lin, Y., Bai, G., Paverd, A., Dong, J.S., Martin, A.: Smart grid metering networks: a survey on security, privacy and open research issues. IEEE Commun. Surv. Tutor. **21**(3), 2886–2927 (2019)
99. Kurt, M.N., Ogundijo, O., Li, C., Wang, X.: Online cyber-attack detection in smart grid: a reinforcement learning approach. IEEE Trans. Smart Grid **10**(5), 5174–5185 (2018)
100. Kwon, Y., Kim, H.K., Lim, Y.H., Lim, J.I.: A behavior-based intrusion detection technique for smart grid infrastructure. In: 2015 Eindhoven PowerTech, IEEE, pp. 1–6 (2015)
101. Kwon, Y., Lee, S., King, R., Lim, J.I., Kim, H.K.: Behavior analysis and anomaly detection for a digital substation on cyber-physical system. Electronics **8**(3), 326 (2019)
102. Li, M., Zhang, K., Liu, J., Gong, H., Zhang, Z.: Blockchain-based anomaly detection of electricity consumption in smart grids. Pattern Recognit. Lett. **138**, 476–482 (2020)
103. Li, R., Bhattacharjee, S., Das, S.K., Yamana, H.: Look-up table based FHE system for privacy preserving anomaly detection in smart grids. In: 2022 International Conference on Smart Computing (SMARTCOMP), IEEE, pp. 108–115 (2022)
104. Li, S., Pandey, A., Hooi, B., Faloutsos, C., Pileggi, L.: Dynamic graph-based anomaly detection in the electrical grid. IEEE Trans. Power Syst. **37**(5), 3408–3422 (2021)
105. Linda, O., Manic, M., Vollmer, T.: Improving cyber-security of smart grid systems via anomaly detection and linguistic domain knowledge. In: 2012 5th International Symposium on Resilient Control Systems, IEEE, pp. 48–54 (2012)
106. Lipčák, P., Macak, M., Rossi, B.: Big data platform for smart grids power consumption anomaly detection. In: 2019 Federated

Conference on Computer Science and Information Systems (FedCSIS), IEEE, pp. 771–780 (2019)
107. Liu, C.C., Stefanov, A., Hong, J., Panciatici, P.: Intruders in the grid. IEEE Power Energy Mag. **10**(1), 58–66 (2011)
108. Liu, X., Nielsen, P.S.: Regression-based online anomaly detection for smart grid data. (2016) arXiv preprint arXiv:1606.05781
109. Louk, M.H.L., Tama, B.A.: Revisiting gradient boosting-based approaches for learning imbalanced data: a case of anomaly detection on power grids. Big Data Cognit. Comput. **6**(2), 41 (2022)
110. Macola, I.G.: The five worst cyberattacks against the power industry since 2014. (2020) https://www.power-technology.com/features/the-five-worst-cyberattacks-against-the-power-industry-since2014/. Accessed 01 March 2023
111. Madabhushi, S., Dewri, R.: Detection of demand manipulation attacks on a power grid. In: 2021 18th Annual International Conference on Privacy (PST), pp. 1–10. Security and Trust, IEEE (2021)
112. Madabhushi, S., Dewri, R.: On the impact of model tolerance in power grid anomaly detection systems. In: 2022 18th International Conference on Information Systems Security (ICISS), Springer Nature Switzerland, pp. 220–234 (2022)
113. Malhotra, P., Vig, L., Shroff, G., Agarwal, P.: Long short term memory networks for anomaly detection in time series. In: 2015 23rd European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning (ESANN), pp. 89–94 (2015)
114. Mao, W., Cao, X., Yan, T., Zhang, Y.: Anomaly detection for power consumption data based on isolated forest. In: 2018 International Conference on Power System Technology (POWERCON), IEEE, pp. 4169–4174 (2018)
115. Marino, D.L., Wickramasinghe, C.S., Amarasinghe, K., Challa, H., Richardson, P., Jillepalli, A.A., Johnson, B.K., Rieger, C., Manic, M.: Cyber and physical anomaly detection in smart-grids. In: 2019 Resilience Week (RWS), IEEE, vol 1, pp. 187–193 (2019)
116. Marino, D.L., Wickramasinghe, C.S., Rieger, C., Manic, M.: Data-driven stochastic anomaly detection on smart-grid communications using mixture poisson distributions. In: 2019 45th Annual Conference of the IEEE Industrial Electronics Society, IEEE, pp. 5855–5861 (2019)
117. Marnerides, A.K., Smith, P., Schaeffer-Filho, A., Mauthe, A.: Power consumption profiling using energy time-frequency distributions in smart grids. IEEE Commun. Lett. **19**(1), 46–49 (2014)
118. Mashima, D., Cárdenas, A.A.: Evaluating electricity theft detectors in smart grid networks. In: International Workshop on Recent Advances in Intrusion Detection, Springer, pp. 210–229 (2012)
119. Mathur, A., Tippenhauer, N.O.: SWaT: A water treatment testbed for research and training on ics security. In: 2016 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater), pp. 31–36 (2016)
120. Matthews, S.J., Leger, A.S.: Leveraging mapreduce and synchrophasors for real-time anomaly detection in the smart grid. IEEE Trans. Emerg. Top. Comput. **7**(3), 392–403 (2017)
121. Matthews, S.J., Leger, A.S.: Leveraging single board computers for anomaly detection in the smart grid. In: 2017 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), IEEE, pp. 437–443 (2017)
122. Menon, D.M., Radhika, N.: Anomaly detection in smart grid traffic data for home area network. In: 2016 International Conference on Circuit, pp. 1–4. Power and Computing Technologies (ICCPCT), IEEE (2016)
123. Moghaddass, R., Wang, J.: A hierarchical framework for smart grid anomaly detection using large-scale smart meter data. IEEE Trans. Smart Grid **9**(6), 5820–5830 (2017)
124. Mohammadi Rouzbahani, H., Karimipour, H., Rahimnejad, A., Dehghantanha, A., Srivastava, G.: Anomaly detection in cyber-physical systems using machine learning. In: Handbook of Big Data Privacy, Springer, pp. 219–235 (2020)
125. Mookiah, L., Dean, C., Eberle, W.: Graph-based anomaly detection on smart grid data. In: 2017 30th International FLAIRS Conference, pp. 306–311 (2017)
126. Moslemi, R., Davoodi, M., Velni, J.M.: A distributed approach for estimation of information matrix in smart grids and its application for anomaly detection. In: 2020 International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), IEEE, pp. 1–7 (2020)
127. Nam, H.S., Jeong, Y.K., Park, J.W.: An anomaly detection scheme based on LSTM autoencoder for energy management. In: 2020 International Conference on Information and Communication Technology Convergence (ICTC), IEEE, pp. 1445–1447 (2020)
128. Nasr, P.M., Varjani, A.Y.: Alarm based anomaly detection of insider attacks in SCADA system. In: 2014 Smart Grid Conference (SGC), IEEE, pp. 1–6 (2014)
129. National Centers for Environmental Information. Billion-dollar weather and climate disasters: Events. (2021) https://www.ncdc.noaa.gov/billions/events. Accessed 01 March 2023
130. Neverman, A.: When the power grid fails—12 things you need to prepare (2022). https://commonsensehome.com/when-the-power-grid-fails/#Why_Does_The_Grid_Go_Down. Accessed 01 March 2023
131. Nguyen, V.Q., Van Ma, L., Kim, J.y., Kim, K., Kim, J.: Applications of anomaly detection using deep learning on time series data. In: 2018 16th International Conference on Dependable, Autonomic and Secure Computing, 16th International Conference on Pervasive Intelligence and Computing, 4th International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), IEEE, pp. 393–396 (2018)
132. Niu, X., Li, J., Sun, J., Tomsovic, K.: Dynamic detection of false data injection attack in smart grid using deep learning. In: 2019 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference (ISGT), IEEE, pp. 1–6 (2019)
133. Noureen, S.S., Bayne, S.B., Shaffer, E., Porschet, D., Berman, M.: Anomaly detection in cyber-physical system using logistic regression analysis. In: 2019 IEEE Texas Power and Energy Conference (TPEC), IEEE, pp. 1–6 (2019)
134. Olivares-Rojas, J.C., Reyes-Archundia, E., Gutierrez-Gnecchi, J.A., Molina-Moreno, I., Cerda-Jacobo, J., Méndez-Patiño, A.: Towards cybersecurity of the smart grid using digital twins. IEEE Internet Comput. **26**(3), 52–57 (2021)
135. OpenEI. Phasor data concentrator (pdc). (2012) https://openei.org/wiki/Definition:Phasor_Data_Concentrator_(PDC). Accessed 01 March 2023
136. Oprea, S.V., Bâra, A., Puican, F.C., Radu, I.C.: Anomaly detection with machine learning algorithms and big data in electricity consumption. Sustainability **13**(19), 10,963 (2021)
137. Otoum, S., Kantarci, B., Mouftah, H.T.: Mitigating false negative intruder decisions in WSN-based smart grid monitoring. In: 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), IEEE, pp. 153–158 (2017)
138. Ouyang, Z., Sun, X., Yue, D.: Hierarchical time series feature extraction for power consumption anomaly detection. In: Advanced Computational Methods in Energy, Power, Electric Vehicles, and Their Integration, Springer, pp. 267–275 (2017)
139. Ouyang, Z., Sun, X., Chen, J., Yue, D., Zhang, T.: Multi-view stacking ensemble for power consumption anomaly detection in the context of industrial internet of things. IEEE Access **6**, 9623–9631 (2018)
140. Pagliery, J.: Hackers attacked the U.S. energy grid 79 times this year. (2014) https://money.cnn.com/2014/11/18/technology/security/energy-grid-hack/. Accessed 01 March 2023

141. Pan, K., Palensky, P., Esfahani, P.M.: From static to dynamic anomaly detection with application to power system cyber security. IEEE Trans. Power Syst. **35**(2), 1584–1596 (2019)
142. Panthi, M.: Anomaly detection in smart grids using machine learning techniques. In: 2020 First International Conference on Power, Control and Computing Technologies (ICPC2T), IEEE, pp. 220–222 (2020)
143. Parsai, S., Mahajan, S.: Anomaly Detection Using Long Short-Term Memory. In: 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), IEEE, pp. 333–337 (2020)
144. Parthasarathy, S., Kundur, D.: Bloom filter based intrusion detection for smart grid SCADA. In: 2012 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), pp. 1–6 (2012)
145. Passerini, F., Tonello, A.M.: Smart grid monitoring using power line modems: anomaly detection and localization. IEEE Trans. Smart Grid **10**(6), 6178–6186 (2019)
146. Pereira, J., Silveira, M.: Unsupervised anomaly detection in energy time series data using variational recurrent autoencoders with attention. In: 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA), IEEE, pp. 1275–1282 (2018)
147. Pliatsios, D., Sarigiannidis, P., Liatifis, T., Rompolos, K., Siniosoglou, I.: A novel and interactive industrial control system honeypot for critical smart grid infrastructure. In: 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), IEEE, pp. 1–6 (2019)
148. Pliatsios, D., Sarigiannidis, P., Lagkas, T., Sarigiannidis, A.G.: A survey on SCADA systems: secure protocols, incidents, threats and tactics. IEEE Commun. Surv. Tutor. **22**(3), 1942–1976 (2020)
149. Promper, C., Engel, D., Green, R.C.: Anomaly detection in smart grids with imbalanced data methods. In: 2017 IEEE Symposium Series on Computational Intelligence (SSCI), IEEE, pp. 1–8 (2017)
150. Qi, R., Rasband, C., Zheng, J., Longoria, R.: Detecting cyber attacks in smart grids using semi-supervised anomaly detection and deep representation learning. Information **12**(8), 328 (2021)
151. Qiu, H., Tu, Y., Zhang, Y.: Anomaly detection for power consumption patterns in electricity early warning system. In: 2018 10th International Conference on Advanced Computational Intelligence (ICACI), IEEE, pp. 867–873 (2018)
152. Qu, Z., Liu, H., Wang, Z., Xu, J., Zhang, P., Zeng, H.: A combined genetic optimization with AdaBoost ensemble model for anomaly detection in buildings electricity consumption. Energy Build. **248**(111), 193 (2021)
153. Rahimi, A., Shahrestani, A., Ramezani, S., Zamani, P., Tehrani, S.O., Moghaddam, M.H.Y.: Filter based time-series anomaly detection in AMI using AI approaches. In: 2021 5th International Conference on Internet of Things and Applications (IoT), IEEE, pp. 1–6 (2021)
154. Raman, G., Peng, J.C.H., Rahwan, T.: Manipulating residents' behavior to attack the urban power distribution system. IEEE Trans. Ind. Inf. **15**(10), 5575–5587 (2019)
155. Raman, G., AlShebli, B., Waniek, M., Rahwan, T., Peng, J.C.H.: How weaponizing disinformation can bring down a city's power grid. PLoS ONE **15**(8), 1–14 (2020)
156. Rashid, H., Singh, P.: Monitor: An abnormality detection approach in buildings energy consumption. In: 2018 4th International Conference on Collaboration and Internet Computing (CIC), IEEE, pp. 16–25 (2018)
157. Rashid, H., Arjunan, P., Singh, P., Singh, A.: Collect, compare, and score: a generic data-driven anomaly detection method for buildings. In: 2016 7th International Conference on Future Energy Systems Poster Sessions, pp. 1–2 (2016)
158. Rashid, H., Stankovic, V., Stankovic, L., Singh, P.: Evaluation of non-intrusive load monitoring algorithms for appliance-level anomaly detection. In: 2019 International Conference on Acoustics, pp. 8325–8329. Speech and Signal Processing (ICASSP), IEEE (2019)
159. Ravikumar, G., Govindarasu, M.: Anomaly detection and mitigation for wide-area damping control using machine learning. IEEE Trans. Smart Grid (2020)
160. Rawat, D.B., Bajracharya, C.: Detection of false data injection attacks in smart grid communication systems. IEEE Signal Process. Lett. **22**(10), 1652–1656 (2015)
161. Rawat, S.S., Polavarapu, V.A., Kumar, V., Aruna, E., Sumathi, V.: Anomaly detection in smart grid using rough set theory and K cross validation. In: 2014 International Conference on Circuits, pp. 479–483. Power and Computing Technologies (ICCPCT), IEEE (2014)
162. Ren, W., Yardley, T., Nahrstedt, K.: Edmand: Edge-based multi-level anomaly detection for SCADA networks. In: 2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), IEEE, pp. 1–7 (2018)
163. Reuter, L., Jung, O., Magin, J.: Neural network based anomaly detection for SCADA systems. In: 2020 23rd Conference on Innovation in Clouds, pp. 194–201. Internet and Networks and Workshops (ICIN), IEEE (2020)
164. Rid, T.: Cyber war will not take place. J. Strateg. Stud. **35**(1), 5–32 (2012)
165. Rossi, B., Chren, S., Buhnova, B., Pitner, T.: Anomaly detection in smart grid data: an experience report. In: 2016 International Conference on Systems, Man, and Cybernetics (SMC), IEEE, pp. 002313–002318 (2016)
166. Ruben, C., Dhulipala, S., Nagaraj, K., Zou, S., Starke, A., Bretas, A., Zare, A., McNair, J.: Hybrid data-driven physics model-based framework for enhanced cyber-physical smart grid security. IET Smart Grid **3**(4), 445–453 (2020)
167. Rubin, F.P., de Souza, P.S.S., dos Santos Marques, W., de Oliveira, R.R., Rossi, F.D., Ferreto, T.: Evaluating energy and thermal efficiency of anomaly detection algorithms in edge devices. In: 2020 International Conference on Information Networking (ICOIN), IEEE, pp. 208–213 (2020)
168. Rösch, D., Ruhe, S., Schäfer, K., Nicolai, S.: Local anomaly detection analysis in distribution grid based on IEC 61850-9-2 LE SV voltage signals. In: 2019 International Conference on Smart Energy Systems and Technologies (SEST), IEEE, pp. 1–6 (2019)
169. Saad, A., Sisworahardjo, N.: Data analytics-based anomaly detection in smart distribution network. In: 2017 International Conference on High Voltage Engineering and Power Systems (ICHVEPS), IEEE, pp. 1–5 (2017)
170. Sahani, N., Zhu, R., Cho, J.H., Liu, C.C.: Machine learning-based intrusion detection for smart grid computing: a survey. ACM Transactions on Cyber-Physical Systems (2023)
171. Sahu, N.K., Mukherjee, I.: Machine learning based anomaly detection for IoT network. In: 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI), IEEE, pp. 787–794 (2020)
172. Sakhnini, J., Karimipour, H., Dehghantanha, A., Parizi, R.M., Srivastava, G.: Security aspects of internet of things aided smart grids: a bibliometric survey. Internet Things **14**(100), 111 (2021)
173. Saraswat, D., Bhattacharya, P., Zuhair, M., Verma, A., Kumar, A.: Ansmart: A SVM-based anomaly detection scheme via system profiling in smart grids. In: 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), IEEE, pp. 417–422 (2021)
174. Serrano-Guerrero, X., Escrivá-Escrivá, G., Luna-Romero, S., Clairand, J.M.: A time-series treatment method to obtain elec-

trical consumption patterns for anomalies detection improvement in electrical consumption profiles. Energies **13**(5), 1046 (2020)
175. Shabad, P.K.R., Alrashide, A., Mohammed, O.: Anomaly detection in smart grids using machine learning. In: 2021 47th Annual Conference of the IEEE Industrial Electronics Society (IECON), IEEE, pp. 1–8 (2021)
176. Shin, D.H., Zhang, J.: Early anomaly detection in an interconnected power grid and communication network: Exploiting interdependent structure of failures. In: 2015 IEEE Global Communications Conference (GLOBECOM), IEEE, pp. 1–6 (2015)
177. Shouyu, L., Zhang, K., Fang, W., Zhou, Z., Hu, R., Zhu, W., Li, Y., Wang, Y., Hou, J.: Anomaly detection of power grid dispatching platform based on isolation forest and K-means fusion algorithm. J. Phys: Conf. Ser. **1601**(2), 022,010 (2020)
178. Shylendra, A., Shukla, P., Mukhopadhyay, S., Bhunia, S., Trivedi, A.R.: Low power unsupervised anomaly detection by nonparametric modeling of sensor statistics. IEEE Trans. Very Large Scale Integr. VLSI Syst. **28**(8), 1833–1843 (2020)
179. Singh, S., Bhardwaj, S., Pandey, H., Beniwal, G.: Anomaly detection using federated learning. In: 2021 International Conference on Artificial Intelligence and Applications, Springer, pp. 141–148 (2021)
180. Singh, V.K., Govindarasu, M.: Decision tree based anomaly detection for remedial action scheme in smart grid using pmu data. In: 2018 IEEE Power and Energy Society General Meeting (PESGM), IEEE, pp. 1–5 (2018)
181. Singh, V.K., Govindarasu, M.: A cyber-physical anomaly detection for wide-area protection using machine learning. IEEE Trans. Smart Grid **12**(4), 3514–3526 (2021)
182. Singh, V.K., Ozen, A., Govindarasu, M.: A hierarchical multi-agent based anomaly detection for wide-area protection in smart grid. In: 2018 Resilience Week (RWS), IEEE, pp. 63–69 (2018)
183. Siniosoglou, I., Efstathopoulos, G., Pliatsios, D., Moscholios, I.D., Sarigiannidis, A., Sakellari, G., Loukas, G., Sarigiannidis, P.: Neuralpot: an industrial honeypot implementation based on deep neural networks. In: 2020 IEEE Symposium on Computers and Communications (ISCC), IEEE, pp. 1–7 (2020)
184. 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. Manage. **18**(2), 1137–1151 (2021)
185. Sisworahardjo, N., Saad, A.A.: Spatio-temporal context anomaly detection for residential power consumption. Int. J. Electr. Eng. Inform. **9**(4), 776–785 (2017)
186. Skopik, F., Friedberg, I., Fiedler, R.: Dealing with advanced persistent threats in smart grid ICT networks. In: 2014 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference (ISGT), IEEE, pp. 1–5 (2014)
187. Soltan, S., Mittal, P., Poor, H.V.: BlackIoT: IoT botnet of high wattage devices can disrupt the power grid. In: 2018 27th USENIX Security Symposium, pp. 15–32 (2018)
188. Starke, A., McNair, J., Trevizan, R., Bretas, A., Peeples, J., Zare, A.: Toward resilient smart grid communications using distributed SDN with ML-based anomaly detection. In: 2018 International Conference on Wired/Wireless Internet Communication, Springer, pp. 83–94 (2018)
189. Steiger, M., Bernard, J., Mittelstädt, S., Lücke-Tieke, H., Keim, D., May, T., Kohlhammer, J.: Visual analysis of time-series similarities for anomaly detection in sensor networks. Comput. Graph. Forum **33**(3), 401–410 (2014)
190. Storm, J.M., Hagen, J., Toftegaard, ØA.A.: A survey of using process data and features of industrial control systems in intrusion detection. In: 2021 IEEE International Conference on Big Data (Big Data), IEEE, pp. 2170–2177 (2021)
191. Sun, M., Zhang, J.: Data-driven anomaly detection in modern power systems. In: Srikantha, P., Farag, H., Wei-Kocsis, J., Karimipour H. (eds.). Security of Cyber-Physical Systems, Springer, pp. 131–143 (2020)
192. Takiddin, A., Ismail, M., Zafar, U., Serpedin, E.: Deep autoencoder-based anomaly detection of electricity theft cyber-attacks in smart grids. IEEE Syst. J. (2022)
193. Ten, C.W., Hong, J., Liu, C.C.: Anomaly detection for cybersecurity of the substations. IEEE Trans. Smart Grid **2**(4), 865–873 (2011)
194. Theumer, P., Zeiser, R., Trauner, L., Reinhart, G.: Anomaly detection on industrial time series for retaining energy efficiency. Procedia CIRP **99**, 33–38 (2021)
195. Thompson, D., Wang, H.: Integrated power signature generation circuit for iot abnormality detection. ACM J. Emerg. Technol. Comput. Syst. 18(1):1–13 (2021)
196. Toshpulatov, M., Zincir-Heywood, N.: Anomaly detection on smart meters using hierarchical self organizing maps. In: 2021 Canadian Conference on Electrical and Computer Engineering (CCECE), IEEE, pp. 1–6 (2021)
197. Tsukada, M., Kondo, M., Matsutani, H.: A neural network-based on-device learning anomaly detector for edge devices. IEEE Trans. Comput. **69**(7), 1027–1044 (2020)
198. US Government Accountability Office. Electricity grid cybersecurity (2021). https://www.gao.gov/products/gao-21-81. Accessed 01 March 2023
199. Utomo, D., Hsiung, P.A.: Anomaly detection at the IoT edge using deep learning. In: 2019 International Conference on Consumer Electronics-Taiwan (ICCE-TW), IEEE, pp. 1–2 (2019)
200. Valdes, A., Macwan, R., Backes, M.: Anomaly detection in electrical substation circuits via unsupervised machine learning. In: 2016 17th International Conference on Information Reuse and Integration (IRI), IEEE, pp. 500–505 (2016)
201. Valenzuela, J., Wang, J., Bissinger, N.: Real-time intrusion detection in power system operations. IEEE Trans. Power Syst. **28**(2), 1052–1062 (2012)
202. Wan Yen, S., Morris, S., Ezra, M.A., Jun Huat, T.: 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. **109**, 1–8 (2019)
203. Wang, D., Wang, X., Zhang, Y., Jin, L.: Detection of power grid disturbances and cyber-attacks based on machine learning. J. Inf. Secur. Appl. **46**, 42–52 (2019)
204. Wang, P., Govindarasu, M.: Cyber-physical anomaly detection for power grid with machine learning. In: Industrial Control Systems Security and Resiliency, Springer, pp. 31–49 (2019)
205. Wang, P., Govindarasu, M.: Cyber-Physical Anomaly Detection for Power Grid with Machine Learning, pp. 31–49. Springer, Cham (2019)
206. Wang, P., Govindarasu, M.: Multi-agent based attack-resilient system integrity protection for smart grid. IEEE Trans. Smart Grid **11**(4), 3447–3456 (2020)
207. Wang, Q., Tai, W., Tang, Y., Ni, M.: Review of the false data injection attack against the cyber-physical power system. IET Cyber-Phys. Syst. Theory Appl. **4**(2), 101–107 (2019-06)
208. Wang, X., Ahn, S.H.: Real-time prediction and anomaly detection of electrical load in a residential community. Appl. Energy **259**, 114,145 (2020)
209. Wang, X., Yang, I., Ahn, S.H.: Sample efficient home power anomaly detection in real time using semi-supervised learning. IEEE Access **7**, 139,712-139,725 (2019)
210. Wang, X., Zhao, T., Liu, H., He, R.: Power consumption predicting and anomaly detection based on long short-term memory neural network. In: 2019 4th International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), IEEE, pp. 487–491 (2019)
211. Wang, Z., Fu, Y., Song, C., Zeng, P., Qiao, L.: Power system anomaly detection based on OCSVM optimized by improved

particle swarm optimization. IEEE Access **7**, 181,580-181,588 (2019)
212. Wei, Q., Ma, R., Wang, Y., Chen, M., Sun, Y., Liu, M., Lin, X.: Glad: A method of microgrid anomaly detection based on esd in smart power grid. In: 2020 International Conference on Power, pp. 103–107. Intelligent Computing and Systems (ICPICS), IEEE (2020)
213. Weiss, M., Weiss, M.: An assessment of threats to the American power grid. Energy Sustain. Soc. **9**(18), 1–9 (2019)
214. Wikipedia. Electricity grid simple- North America.svg. (2008) https://commons.wikimedia.org/wiki/File:Electricity_grid_simple-_North_America.svg. Accessed 01 March 2023
215. Wilson, D., Tang, Y., Yan, J., Lu, Z.: Deep learning-aided cyber-attack detection in power transmission systems. In: 2018 IEEE Power and Energy Society General Meeting (PESGM), IEEE, pp. 1–5 (2018)
216. Wu, J., Xiong, J., Shil, P., Shi. Y.: Real time anomaly detection in wide area monitoring of smart grids. In: 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), IEEE, pp. 197–204 (2014)
217. Xiang, B., Liu, Z., Zhang, K.: Flagging implausible inspection reports of distribution transformers via anomaly detection. IEEE Access **8**, 75,798-75,808 (2020)
218. Xiang, Y., Wang, L., Liu, N.: Coordinated attacks on electric power systems in a cyber-physical environment. Electr. Power Syst. Res. **149**, 156–168 (2017)
219. Xiao, Yj., Xu, Wy., Jia, Zh., Ma, Zr., Dl, Qi.: NIPAD: a non-invasive power-based anomaly detection scheme for programmable logic controllers. Front. Inf. Technol. Electron. Eng. **18**(4), 519–534 (2017)
220. Xu, A., Jiang, Y., Cao, Y., Zhang, G., Ji, X., Xu, W.: ADDP: anomaly detection for DTU based on power consumption side-channel. In: 2019 3rd Conference on Energy Internet and Energy System Integration (EI2), IEEE, pp. 2659–2663 (2019)
221. Xu, A., Wu, T., Zhang, Y., Hu, Z., Jiang, Y.: Graph-based time series edge anomaly detection in smart grid. In: 2021 7th International Conference on Big Data Security on Cloud (BigDataSecurity), International Conference on High Performance and Smart Computing, (HPSC) and International Conference on Intelligent Data and Security (IDS), IEEE, pp. 1–6 (2021)
222. Xu, C., Chen, H.: A hybrid data mining approach for anomaly detection and evaluation in residential buildings energy data. Energy Buildings **215**, 109,864 (2020)
223. Xu, C., Wang, J., Zhang, J., Li, X.: Anomaly detection of power consumption in yarn spinning using transfer learning. Comput. Ind. Eng. **152**, 107,015 (2021)
224. Yan, Y., Qian, Y., Sharif, H., Tipper, D.: A survey on smart grid communication infrastructures: motivations, requirements and challenges. IEEE Commun. Surv. Tutor. **15**(1), 5–20 (2012)
225. Yang, L., Li, F.: Detecting false data injection in smart grid in-network aggregation. In: 2013 IEEE International Conference on Smart Grid Communications (SmartGridComm), IEEE, pp. 408–413 (2013)
226. Yang, Y., Littler, T., Sezer, S., McLaughlin, K., Wang, H.F.: Impact of cyber-security issues on smart grid. In: 2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies, IEEE, pp. 1–7 (2011)
227. 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. **109**, 1–8 (2019)
228. Yijia, T., Hang, G.: Anomaly detection of power consumption based on waveform feature recognition. In: 2016 11th International Conference on Computer Science and Education (ICCSE), IEEE, pp. 587–591 (2016)
229. Yip, S.C., Tan, W.N., Tan, C., Gan, M.T., Wong, K.: An anomaly detection framework for identifying energy theft and defective meters in smart grids. Int. J. Electr. Power Energy Syst. **101**, 189–203 (2018)
230. Yu, J., Cheng, H., Zhang, J., Li, Q., Wu, S., Zhong, W., Ye, J., Song, W., Ma, P.: CONGO^2: scalable online anomaly detection and localization in power electronics networks. IEEE Internet Things J. **9**(15), 13,862-13,875 (2022)
231. Yuan, Y., Jia, K.: A distributed anomaly detection method of operation energy consumption using smart meter data. In: 2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), IEEE, pp. 310–313 (2015)
232. Yïlmaz, Y., Uludag, S.: Timely detection and mitigation of IoT-based cyberattacks in the smart grid. J. Frankl. Inst. **358**(1), 172–192 (2021)
233. Zhang, J.E., Wu, D., Boulet, B.: Time series anomaly detection for smart grids: a survey. In: 2021 IEEE Electrical Power and Energy Conference (EPEC), IEEE, pp. 125–130 (2021)
234. Zhang, L., Lv, Z., Zhang, X., Chen, C., Li, N., Li, Y., Wang, W.: A novel approach for traffic anomaly detection in power distributed control system and substation system. In: 2019 International Conference on Network and System Security, Springer, pp. 408–417 (2019)
235. Zhang, L., Shen, X., Zhang, F., Ren, M., Ge, B., Li, B.: Anomaly detection for power grid based on time series model. In: 2019 International Conference on Computational Science and Engineering (CSE) and International Conference on Embedded and Ubiquitous Computing (EUC), IEEE, pp. 188–192 (2019)
236. Zhang, L., Wan, L., Xiao, Y., Li, S., Zhu, C.: Anomaly detection method of smart meters data based on GMM-LDA clustering feature learning and PSO support vector machine. In: 2019 Sustainable Power and Energy Conference (ISPEC), IEEE, pp. 2407–2412 (2019)
237. Zhang, Q., Wan, S., Wang, B., Gao, D.W., Ma, H.: Anomaly detection based on random matrix theory for industrial power systems. J. Syst. Architect. **95**, 67–74 (2019)
238. Zhang, Y., Chen, W., Black, J.: Anomaly detection in premise energy consumption data. In: 2011 Power and Energy Society General Meeting, IEEE, pp. 1–8 (2011)
239. Zhao, H., Liu, H., Hu, W., Yan, X.: Anomaly detection and fault analysis of wind turbine components based on deep learning network. Renew. Energy **127**, 825–834 (2018)
240. Zhao, J., Wang, J., Yin, L.: Detection and control against replay attacks in smart grid. In: 2016 12th International Conference on Computational Intelligence and Security (CIS), IEEE, pp. 624–627 (2016)
241. Zhou, F., Wen, G., Ma, Y., Geng, H., Huang, R., Pei, L., Yu, W., Chu, L., Qiu, R.: A comprehensive survey for deep-learning-based abnormality detection in smart grids with multimodal image data. Appl. Sci. **12**(11), 5336 (2022)

242. Zhou, M., Musilek, P.: Real-time anomaly detection in distribution grids using long short term memory network. In: 2021 IEEE Electrical Power and Energy Conference (EPEC), IEEE, pp. 208–213 (2021)
243. Zhou, M., Wang, Y., Srivastava, A.K., Wu, Y., Banerjee, P.: Ensemble-based algorithm for synchrophasor data anomaly detection. IEEE Trans. Smart Grid **10**(3), 2979–2988 (2018)