energies

Review

A Review of AI-Based Cyber-Attack Detection and Mitigation in Microgrids

Omar A. Beg [1,*,†], Asad Ali Khan [2,†], Waqas Ur Rehman [3] and Ali Hassan [4]

[1] Department of Electrical Engineering, The University of Texas Permian Basin, Odessa, TX 79762, USA
[2] Department of Electrical and Computer Engineering, The University of Texas at San Antonio, San Antonio, TX 78249, USA; asad.khan@my.utsa.edu
[3] Department of Electrical and Computer Engineering, Missouri University of Science and Technology, Rolla, MO 65409, USA; w.rehman@mst.edu
[4] Department of Electrical and Computer Engineering, University of Michigan, Dearborn, MI 48126, USA; alihssn@umich.edu
[*] Correspondence: beg_o@utpb.edu
[†] These authors contributed equally to this work.

Abstract: In this paper, the application and future vision of Artificial Intelligence (AI)-based techniques in microgrids are presented from a cyber-security perspective of physical devices and communication networks. The vulnerabilities of microgrids are investigated under a variety of cyber-attacks targeting sensor measurements, control signals, and information sharing. With the inclusion of communication networks and smart metering devices, the attack surface has increased in microgrids, making them vulnerable to various cyber-attacks. The negative impact of such attacks may render the microgrids out-of-service, and the attacks may propagate throughout the network due to the absence of efficient mitigation approaches. AI-based techniques are being employed to tackle such data-driven cyber-attacks due to their exceptional pattern recognition and learning capabilities. AI-based methods for cyber-attack detection and mitigation that address the cyber-attacks in microgrids are summarized. A case study is presented showing the performance of AI-based cyber-attack mitigation in a distributed cooperative control-based AC microgrid. Finally, future potential research directions are provided that include the application of transfer learning and explainable AI techniques to increase the trust of AI-based models in the microgrid domain.

Keywords: cyber-attacks; false data injection;microgrids; artificial intelligence; detection; mitigation; neural networks; smart grids

check for updates

Citation: Beg, O.A.; Khan, A.A.; Rehman, W.U.; Hassan, A. A Review of AI-Based Cyber-Attack Detection and Mitigation in Microgrids. *Energies* **2023**, *16*, 7644. https://doi.org/10.3390/en16227644

Academic Editor: José Matas

Received: 13 October 2023
Revised: 13 November 2023
Accepted: 15 November 2023
Published: 18 November 2023

1. Introduction

A microgrid is a group of interconnected loads and distributed energy resources (DERs) that supply power to local customers and can operate in either islanded or grid-connected mode. Microgrids are being leveraged to achieve economic operation, sustainable energy, and resilient power provision objectives [1–4]. The microgrid's controller orchestrates multiple DERs and controllable loads to provide clean and reliable energy at economical prices. As shown in Figure 1, a typical hierarchical control architecture consists of three layers that operate at varying time scales to achieve the control objectives [5]. The secondary control layer is vital to maintain voltage and frequency at nominal values in islanded operating mode and, in contrast to centralized control, the distributed secondary control offers flexible, reliable, and seamless integration of DERs [6–8].

Modern microgrids have transformed into cyber-physical systems where physical assets such as DERs, loads, and power electronics devices make the physical layer and the cyber layer constitutes a communication network and software-based controllers [9]. As a result of their reliance on the Internet of Things (IoT) and newly developed wide-area sensor networks, microgrids are particularly vulnerable to cyber-attacks and network outages. Examples of real-world network failures include North America (2003), which experienced a problem with the status estimator and alarm system, Austria (2013), which experienced network congestion as a result of a software defect, and Switzerland (2005), which experienced information overload. Due to a cyber-attack brought on by malware known as BlackEnergy in control center computers, Ukraine's power infrastructure failed in December 2015, knocking out thousands of homes and facilities. A significant percentage of consumers would lose power due to such malfunctions and cyber-attacks, and very sensitive and mission-critical equipment may suffer serious harm [10–15].

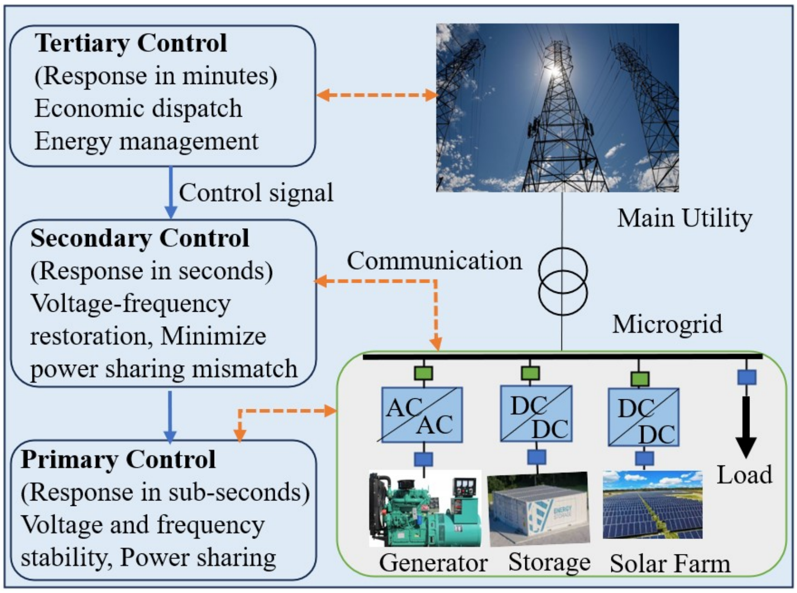


Figure 1. The hierarchical control structure operates at three levels to meet the microgrid's operator objectives.

Table 1 summarizes the actual reported cyber-attacks on the energy industry [16–18]. After examining reported cyber-attacks on the energy sector, a typical cyber-attack chain is found to be initiated by gaining initial access through spear phishing. After gaining an initial foothold, adversaries perform a reconnaissance of the network data to spread out and exfiltrate critical information. Once suspicious logins are established, the attackers manipulate the control and safety systems by dispatching malicious commands and locking out the operators from their machines [19]. The extensive communication network-based cyber layer has resulted in an increased attack surface in microgrids, making them vulnerable to cyber-attacks [20]. As shown in Figure 2, such cyber-attacks may target information sharing among the microgrid's controller and various intelligent electronic devices (IEDs) by either manipulating the measurements or causing communication delays [21,22]. Attackers with malicious intent can disrupt the transfer of information, resulting in power outages, financial loss, and system instability. With the development of smart grids and the growing interconnection of communication networks, significant cyber-security risks are affecting power grids [23,24]. With the inclusion of cutting-edge communication and computing tools, the current electricity networks are evolving into smarter systems with increased efficiency. However, because there are so many intelligent devices connected via communication networks, it has led to significant concerns about cyber security. A modern power system's ability to operate reliably and securely is directly impacted by cyber-attacks on such devices. Man-in-the-middle, distributed denial of service, jamming, and false data injection are some of the main types of cyber-attacks that target smart grids [25–27].

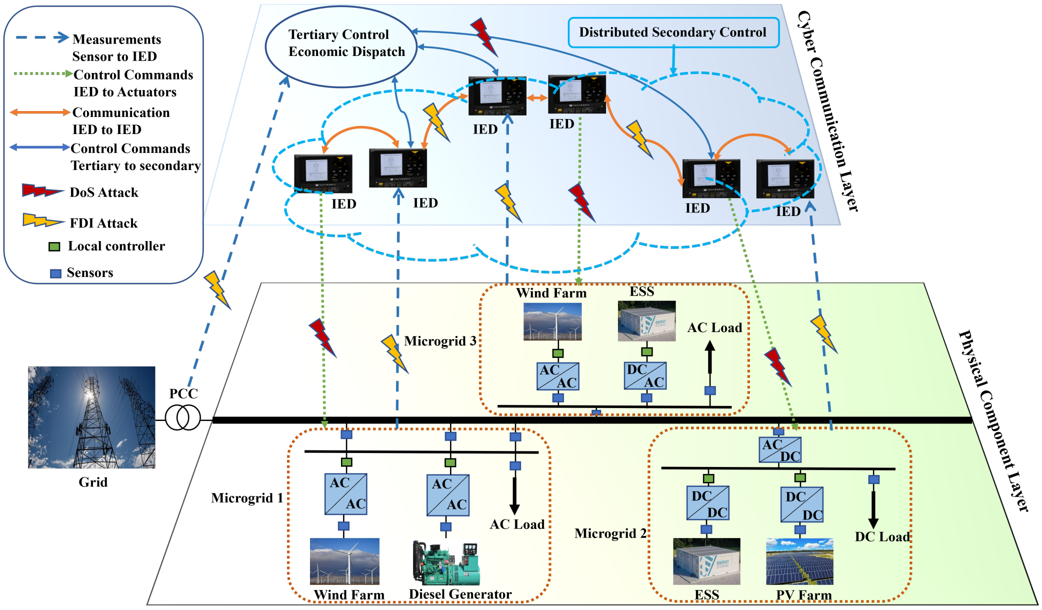


Figure 2. A network of microgrids' architecture with potential cyber-attack targets is shown. Microgrids connect with the main electrical utility at the point of common coupling (PCC). The converters are controlled locally in the physical layers using the primary level control. The distributed secondary-level control implements the control objective that is received from the tertiary-level controller. IED sensor measurements and communications are susceptible to false data injection (FDI) attacks, while denial of service (DoS) attacks could target the control signals being delivered to the actuators.

Table 1. A summary of major cyber-attacks against the energy industry is provided.

Location	Target	Type	Impact
North America (2003)	Network failures in control room operating system	Denial of service	Blackout across multiple regions
Korea Hydro and Nuclear Power (2014)	Unauthorized access to critical information	Potential loss of confidential information and designs	Compromised security and safety of plant and personnel
Ukraine (2015)	BackEnergy malware in control room computers	Denial of service, False data injection	Blackout across multiple substations
Kyiv (2016)	Industroyer malware targeting industrial control systems	Denial of service, Issuing false control commands	Power outage to at least one-fifth of Kyiv
Middle East petrochemical plant (2017)	Safety system of the plant	Potential denial of services and life loss	Plant shut down

IoT networks and devices are rapidly evolving, producing massive volumes of data that require rigorous authentication and security. One of the most promising approaches for addressing cybersecurity risks and providing security is artificial intelligence (AI). AI technology appears to be a potential way to improve control, security, and performance in smart grid networks [28,29]. AI-based algorithms are being used in microgrids for a range of applications including intelligent control designs, forecasting, and cyber-attack identification and mitigation [30–33]. Data-driven methods are being used to predict the availability of renewable resources. The seasonal dependency of solar and wind along with load demand is forecast using various ensemble learning methods. This information helps in power system planning and unit commitment decisions [34,35]. Power system operations can experience interruptions due to power system faults and cyber-attacks. Under such scenarios, the restoration time depends upon the nature and location of a cyber-attack. Modern distributed power systems are equipped with communication layers that accelerate the propagation of such attacks. The AI-based learning algorithms can localize and identify the type of such attack. This helps to reduce the restoration time of compromised systems [36–41]. The power grid resilience can be estimated by the frequency and duration of power outage events. The availability of active and reactive power from each generating unit can be adversely affected if control and communication infrastructure are compromised. AI-based resilient control architectures can improve the reliability of the power network. The learning capabilities of artificial neural networks can mitigate the effects of cyber-attacks [42–46].

Microgrids need to be robust and dependable to deliver a continuous and uninterrupted power supply. Communication networks are necessary for microgrids to coordinate and manage DERs. Microgrids can be efficiently managed by distributed cooperative control strategies, which rely upon real-time monitoring, communication protocols, and interoperability to enable the smooth integration of various microgrid components. Cyberattacks have the potential to compromise security and interrupt regular operations of microgrid control systems. Adversaries might use communication network vulnerabilities to their advantage to intercept or modify the transfer of data. Comprehensive safety precautions need to be taken to stop hostile interference, unauthorized access, and manipulation of control signals. In an ever-evolving environment of cybersecurity threats, regular upgrades, monitoring, and adherence to cybersecurity, best practices are crucial to the optimal operation of microgrids [47–50].

The learning capability of AI-based techniques enables them to estimate the parameters of complex systems, making them suitable for microgrid applications. Various types of artificial neural networks (ANNs), such as the adaptive linear neuron, multi-layer perceptron, feed-forward neural network, Elman neural network, radial basis function network, general regression neural network, and deep neural networks, are in use to design resilient control for microgrids to withstand cyber-attacks [51]. This work specifically focuses on AI-based techniques for cyber-attack detection and mitigation in microgrids. Some of the main contributions of this work are as follows:

1. We conducted a systematic search across several scholarly databases, including Google Scholar, IEEE, MDPI, Elsevier, and Springer, using a combination of keywords and focused search terms associated with our area of study. We focused on peer-reviewed books, journals, conference proceedings, and industry white papers to cover a broad spectrum of perspectives and findings, as shown in Figure 3.
2. The existing techniques are divided into two main categories, i.e., cyber attack detection and mitigation. The system under study, attack type, data acquisition, and training method of AI-based techniques are summarized in tables for each category.
3. A case study is presented on the use case of AI-based technique in the microgrid.

The rest of the paper is organized into 8 sections. The attack surface in modern power systems is expanding with the inclusion of communication networks and intelligent control design. Adversaries can take advantage of various vulnerabilities in microgrids to initiate malicious cyber-attacks. Therefore, Section 2 covers various types of cyber-attacks targeting microgrids. There are several advantages of using intelligent cyber-attack defense strategies, such as early detection of cyber-attacks before they can cause significant damage or disruption to the system, less manual intervention, and enhanced understanding of the system to identify areas for improvement. Hence, cyber-attack detection using AI-based techniques in microgrids is described in Section 3, and Section 4 contains cyber-attack mitigation using AI-based techniques. Learning-based AI techniques are discussed in Section 5. In Section 6, a case study of a test microgrid is presented. The proposed control technique utilizes an advanced AI-based tool tailored to mitigate the data-driven cyber anomalies targeting the communication network of the microgrid. Also, it is scalable and depicts improved performance under complex real-time test scenarios. In Section 7, some challenges and future directions are discussed and, finally, Section 8, concludes this work.

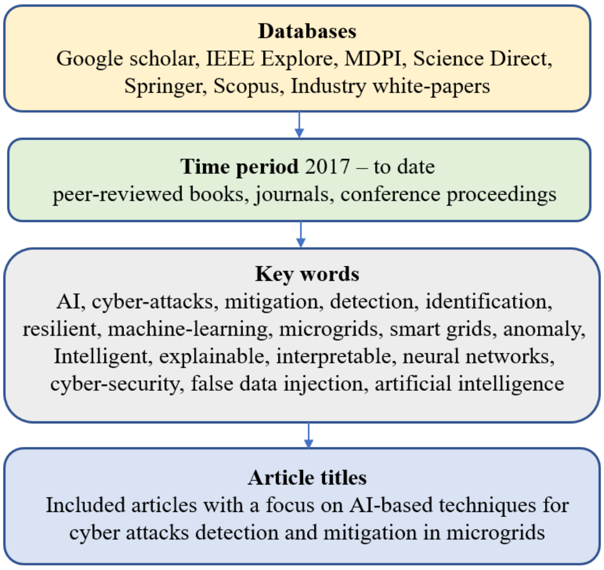

Databases
Google scholar, IEEE Explore, MDPI, Science Direct, Springer, Scopus, Industry white-papers
Time period 2017 – to date
peer-reviewed books, journals, conference proceedings
Key words
AI, cyber-attacks, mitigation, detection, identification, resilient, machine-learning, microgrids, smart grids, anomaly, Intelligent, explainable, interpretable, neural networks, cyber-security, false data injection, artificial intelligence
Article titles
Included articles with a focus on AI-based techniques for cyber attacks detection and mitigation in microgrids

Figure 3. The flow chart depicts the process of selecting articles for this research.

2. Types of Cyber-Attacks in Microgrids

The integrated architecture and related communication networks of microgrids are particularly susceptible to cyber-attacks. The incorporation of intelligent electronic and information-sharing devices and the lack of thorough security standards might leave them vulnerable to malicious cyber-attacks to take advantage of flaws in the system. The potential for smart grid technologies with scalable solutions directly affects the volume of data flow in terms of increased communication and computational needs.

Microgids' interoperability requires the use of numerous information exchange protocols and communication architectures, which could leave the system prone to cyber-attacks due to insufficient information [52]. Figure 4 depicts several cyber-attacks targeting the cyber and physical layer in a microgrid, and an overview of these types of cyber-attacks targeting microgrids is covered below.

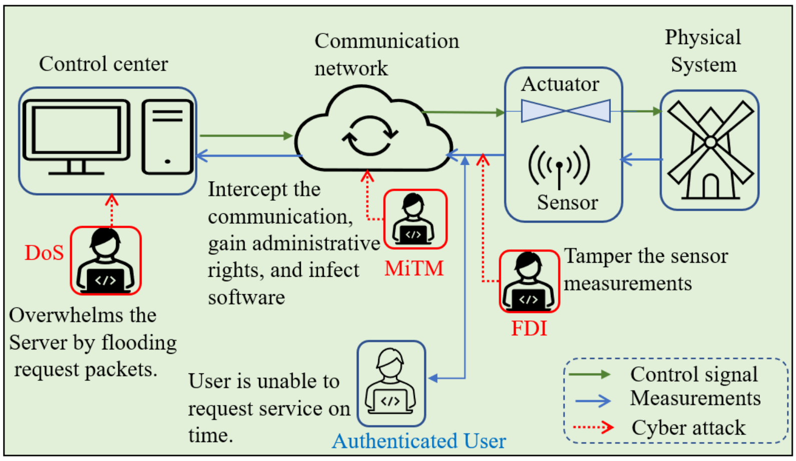

Control center
Communication network
Physical System
Actuator
Sensor
Intercept the communication, gain administrative rights, and infect software
MiTM
DoS
Overwhelms the Server by flooding request packets.
Tamper the sensor measurements
FDI
User is unable to request service on time.
Authenticated User
Control signal
Measurements
Cyber attack

Figure 4. The potential targets of cyber-attacks include the communication networks in the cyber layer and the intelligent devices in the physical layer of the microgrids.

If this issue is not effectively resolved, the system may become more susceptible to cyber-attacks [53].

2.1. False Data Injection Cyber-Attack

False data injection (FDI) is a data-driven attack, in which the attacker may tamper with sensors and phasor measurement units, and compromise the critical information by either injecting false information into the communication network or completely replacing the actual values. This could result in compromised state loss of synchronism and compromised state estimation, which would adversely impact economic dispatch and power supply to critical loads [54,55]. The integrity of the state estimator can be jeopardized by an attacker compromising a subset of meters and sending revised measurements without entirely altering the result. FDI attacks can be carried out even when the attacker is unfamiliar with the power system configuration by obtaining online data, market data, and power flow measurements [56]. Under FDI attack, the feedback signal of a distributed smart grid controller can be described as:

$$U(x_n(t)) = x_n(t) + \phi_n(t), \tag{1}$$

where $U(x_n(t))$ is the feedback signal after false data $\phi_n(t)$ is injected into the nth normal feedback signal of the controller $x_n(t)$. Various types of FDI cyber-attacks, such as periodic, non-periodic, and simultaneous cyber-attacks, can be modeled by updating $\phi_n(t)$ [57]. These FDI attacks also have the potential to undermine or even destroy the distributed control systems that govern modern microgrids. FDI attacks typically change the output of AC microgrids, causing equipment damage, by spoofing communications routes and altering signal levels through a distributed communication network. To prevent the FDI attack from being noticed, the malicious data injection range is chosen inside the range of the nominal working condition of the system. By introducing a variety of false information into the communication network, various FDI attacks can be executed against distributed controller feedback signals [58].

2.2. Denial-of-Service Cyber-Attack

The Denial-of-service (DoS) is a type of cyber-attack that aims to restrict access of an authorized user to a network. Microgrids are becoming a prime target of such DoS cyber-attacks due to their dependency on information sharing to meet control objectives [59]. Such attacks are accomplished by jamming communication lines with inaccurate data and disrupting normal data access between control centers and peripheral devices like sensors and actuators. To carry out these kinds of attacks, one is not required to be familiar with the microgrids' settings or have the necessary skills to alter control messages and measurements. During the DoS cyber-attack on the Ukrainian power grid, operators were unable to communicate control signals to the actuators [10]. Wide area networks can be vulnerable to DoS cyber-attacks if malware is placed in substation routers, giving attackers access to phasor measurement unit (PMU) communications. The reliability of the microgrid is compromised if an attack is successful, since all communication channels must be available for the timely dispatch of control signals. Advanced metering infrastructures may face a cyber threat if an attacker contacts a compromised device after malware has been deployed. By managing a large number of agents, it is possible to deceive the system user into receiving an excessive amount of communication packets. Some of the permitted packets will be lost by the authorized user due to the volume of traffic [53]. In a distributed control-based microgrid with n DERs, the DoS cyber-attack can be modeled as:

$$[\chi_i]_{n\times 1} = \alpha_i(\tau)[\gamma_i]_{n\times 1} + \alpha_j(\tau)[\gamma_j]_{n\times 1}, \tag{2}$$

where χ_i represents one of the compromised target nodes and γ_{ij} are the neighboring nodes of the compromised node. $\alpha_{ij}(\tau)$ are gain factors, $(t_1 < \tau < t_2)$ is the time interval for the occurrence of a malicious cyber-attack, and $ij \in \mathbb{R}$ represents one of the DERs in the microgrid. A gain factor of value (1) means the communication link is compromised and not available, and a gain factor of value (0) means the communication channel is not compromised [57]. The use of data filtering techniques, intrusion detection and prevention systems, and cryptographic authentications can significantly reduce DoS in smart grids by detecting it promptly [60].

2.3. Man-in-the-Middle Cyber-Attack

Man-in-the-Middle (MiTM) cyber-attacks may target the information that devices in the microgrid need to share with one another, including control signals, sensor data, and dispatch commands. Such attacks may also target vital power system components in an effort to intercept and gather information on the communications of control center staff, which may be used to launch more attacks [61]. The attacker can assume the identity of a genuine user, intercept and modify message packets sent between two communication nodes, and insert new message packets, all while remaining undetected. The attacker may establish an illegitimate communication channel between two active nodes and start sending malicious data to modify the communication between the sending and receiving end [62]. To ensure the resilience of the microgrids with an increased attack surface, intelligent technologies must be developed. A great number of bidirectional power electronic converters are essential to the two-way power flow controllability and transactive energy capabilities of modern microgrids. These converters must be adaptable, quick, and durable to support the grid under both normal and compromised operating conditions. The risk of cyber-attacks can be considerably decreased by implementing improved cyber-attack detection and mitigation techniques for microgrids [63].

3. AI-Based Cyber-Attack Detection

The presence of communication networks and smart metering devices in microgrids is generating a large data set. These data sets are enabling increased situational awareness of the microgrids and making them vulnerable to cyber-attacks. Therefore, AI-based techniques are being utilized to detect such data-driven attacks due to their exceptional learning and generalization capabilities [64]. A linear regression-based cyber-attack detection for a distributed control-based islanded DC microgrid is used to detect FDI against voltage and current measurements to maintain a stable control operation [36]. Through their sensors and communication interactions, DC microgrids are vulnerable to cyber-attacks. False data injection into the cyber layer can interfere with control goals, resulting in voltage instability and unbalanced load-sharing patterns. Detection of such attacks is integral to the stable operation of DC microgrids. Therefore, in [37–39], a deep learning-based detection technique is proposed that takes into account the input features, such as the DC bus voltage and the reference voltage, to forecast the duty cycle of the converter. Apart from FDI, Man-in-the-Middle (MiTM), and denial of service (DoS) type cyber-attacks may also target the communication networks due to the interconnected architecture of smart grids. Therefore, deep learning, Naive Bayes, and Random Forest-based detection techniques are proposed in [40,41]. These techniques are trained using supervised learning with real-world operational and network traffic data sets, and showed a higher accuracy rate of above 95% to prevent loss of communication and secure the network and metering data obtained from intelligent electronic devices.

By combining predictions from different models, the machine learning technique known as ensemble learning increases prediction accuracy and robustness. The use of the collective intelligence of the ensemble aims to remove any biases or errors that may occur in individual models [65–67]. Therefore, an ensemble learning-based approach using Decision Trees to detect cyber-attacks on bulk electric power transmission networks targeting bid price and quantity signals is proposed in [68]. This method showed an improved accuracy of 99% to secure the system from attackers to manipulate the system's reliability and make illegitimate profits by compromising electricity pricing contracts. The manipulation of measurements obtained from substations may lead to incorrect power system state estimations in large connected power networks. An ensemble learning-based technique is developed to detect such attacks that give higher accuracy compared to multiple state-of-the-art machine learning-based algorithms in [69]. The data obtained from phasor measurement units in wide area power networks is also a target for data spoofing attacks that may lead to incorrect power system state estimation by compromising the measurement source authentication. Therefore, an ensemble empirical mode decomposition using a back propagation neural network is proposed in [70]. This proposed method is trained using supervised learning with real data from universal grid analyzers from multiple locations and showed improved performance compared to the long short-term memory (LSTM)-based model. Various types of artificial neural networks are being extensively employed for intelligent cyber-attack detection in microgrids. An auto-encoder neural network and a deep learning auto-encoder neural network are used for FDI against load frequency control and voltage sensor measurements in an islanded AC and DC microgrid, respectively [71,72]. Since the auto-encoder neural network can manage undesired input, such as communication channel disruptions, it is often advantageous for microgrid applications. Also, unsupervised learning is utilized in these auto-encoder-based cyber-attack detection techniques to secure communication networks [73]. Recurrent neural networks (RNN) such as LSTM, convolutional neural networks (CNN), and nonlinear auto-regressive exogenous model (NARX) neural networks have shown promising results for cyber-attack detection in microgrids [74–79]. RNNs are a subclass of neural networks that are particularly adept at forecasting time-related data sequences. RNNs permit cyclical connections that can map to each output from prior inputs, in contrast to feed-forward neural networks. The case studies demonstrate that deep RNNs outperform traditional and shallow RNNs and gain from the depth of hidden layers in islanded and grid-connected AC microgrids for FDI and DoS type cyber-attack detection on the communication network and phasor measurements [74,75]. A gated recurrent unit-based neural network and a NARX neural network-based detection techniques against cyber-attacks on current and voltage measurements in an islanded SC microgrid are proposed in [76,80], respectively.

Apart from Deep and recurrent ANNs, classical machine learning methods are widely being used for classification and cyber-attack detection in microgrids such as Logistic regression (LR), k-nearest neighbors (kNN), Gradient boosting (GBT), Random Forest(RF), multi-layer perceptron (MLP), Naive Bayes (NB), and Support vector machines (SVM) [57,81–86]. Tables 2 and 3 summarize the various AI-based cyber-attack detection techniques including the information about data acquisition, training, and performance benchmarking of the proposed methods.

Table 2. Summary of AI-based techniques for cyber-attack detection in microgrids is provided.

System	Attack	Algorithm	Data	Performance Metric
Islanded AC	FDI (control signals, communication networks)	Wavelet transform with deep learning using deep auto-encoder	MATLAB simulations, Unsupervised	Accuracy, >97% [73]
	FDI into load frequency control	Auto-encoder neural network	Using datasets on TensorFlow and Keras software framework, Unsupervised	Not given, [71]
	DoS and FDI into control and measurement signals	Feed-forward ANN, NB, SVM	MATLAB/real-time simulation, Supervised	MAPE [1] 0.6% (FDI), 0.1% (DoS), [57]
	DoS, FDI, and time delay on communication and measurements	LSTM, CNN	Simulation-based data, Supervised	Accuracy nearly 100%, [74]

Table 2. *Cont.*

System	Attack	Algorithm	Data	Performance Metric
Islanded DC	FDI into voltage and current measurements	Linear regression	Simulation-based, Supervised	Not given, [36]
	FDI into output voltage sensor of DC converter	Deep learning	Simulation-based, Supervised using back propagation	Not given, [37]
	FDI into DC bus voltage sensor	Deep learning	Matlab simulation, Supervised	Not given, [38]
	FDI into voltage sensor	Deep learning auto-encoder with grey wolf optimization	Simulation-based, Unsupervised	Precision 95%, [72]
	RL [3]-based intelligent FDI into measurements and control signals	Pattern recognition network, type of feed-forward ANN	Simulation-based, Supervised	Accuracy 98.5%, [81]
	FDI into measurements and communications	NARX ANN	MATLAB/real-time simulations, Supervised	MAPE [1] 0.064% (voltages), 0.36% (currents), [76]
	FDI into sensor, communication network, and measurements	Gated recurrent unit neural network	MATLAB simulation, Supervised	RMSE [2] 0.028036, [80]
Networked	FDI,MiTM, and DoS on network communication	Deep learning	Real data (from smart grid, substation, power plant), Supervised	Accuracy 96.50%, [39]
	FDI into measurements	NB, RF, Regression	Simulation-based, Supervised	F-score (0.08,095,0.81) for (NB, RF, Regression, respectively), [40]
	FDI on substation measurements and sensors	Ensemble learning technique, minimum voting for critical class	Simulation-based, Supervised	Accuracy 98.8%, [69]
	FDI into wide area communication networks and measurements	Deep recurrent ANN	Simulation-based, Supervised	MSE [4] 2.15×10^{-3}, [75]
	FDI and DoS sensor measurements and PV control operation modes	LR, kNN, GBT, RF, MLP	(Real smart home electricity consumption data, real solar power, and MATPOWER simulations), Supervised-based data.	Accuracy 95%, [82]
	FDI and time delay on PV control center	Auto-regressive (AR), data driven approach	Simulation-based, Supervised	Not given, [83]
	FDI into substation measurements, sensors, and control commands	domain-adversarial training based on neural networks (DANN)	Datasets obtained from experimental hardware testbed, Transfer learning	Accuracy 80%, [87]

[1] Mean Absolute Percentage Error, [2] Root Mean Square Error, [3] Reinforcement Learning, [4] Mean Square Error.

Table 3. Continuation of Table 1 (AI-based cyber-attack detection).

System	Attack	Algorithm	Data	Performance Metric
Islanded DC	FDI into currents and voltage measurements	Feed-forward ANN	Real-time Typhoon simulation, supervised	Accuracy >90%, [88]
	FDI into communication network	RNN	MATLAB real-time simulation, Supervised	Not given, [89]

Table 3. *Cont.*

System	Attack	Algorithm	Data	Performance Metric
Islanded AC	FDI into communication layer and replay attacks	NARX ANN	MATLAB real-time simulation, Supervised	Not given, [90]
	FDI into output voltage and power measurements	Deep learning using rectified linear unit	MATLAB simulation, Supervised	Accuracy 91%, [91]
	FDI into measurements	LSTM	MATLAB simulation, Supervised	Not given, [92]
Networked	FDI into substation measurements and sensors	Cross wavelet transform with SVM classifier	Simulation-based, Supervised	Accuracy 95.53%, [84]
	Network traffic attacks (FDI, malware behavior (Dos), Disabling reassembly)	Bidirectional RNN	Normal dataset from operating IEEE 1815.1-based Korean substation and simulations based attacked dataset, Supervised	Accuracy 98%, [77]
	FDI (measurement source data spoofing)	Ensemble empirical mode decomposition using back propagation neural network	Real data from universal grid analyzers in US locations, Supervised	Accuracy 96%, [70]
	FDI (spoofing synchrophasor measurements)	Dynamic dual kernel SVM	distributed Synchrophasor data from FNET/GridEye, (Supervised, particle swarm optimization)	Accuracy 94.26%, [85]
	FDI (spoofing synchrophasor measurements)	Multi-view convolutional neural networks (CNN)	Distributed synchrophasor data from 11 locations in the frequency measurements network FNET/GridEye, Supervised	Accuracy 91.46%, [78]
	FDI into sensor and measurements	Isolation forest based technique	MATPOWER based simulations, Unsupervised	Accuracy 94%, [86]
	FDI, DoS, Distributed DoS on communication networks and sensors	Deep Learning(LSTM,RNN)	MATLAB-based simulation, Supervised	Accuracy 95%, [79]
	FDI into PV related measurements	ANFIS	MATLAB simulation, Supervised	RMSE 0.11, [93]
	DOS, communication layer	Decision Tree classifier	MATLAB simulation, supervised	Accuracy 98%, [94]

4. AI-Based Cyber-Attack Mitigation

With the inclusion of DERs and communication networks, distributed control is becoming popular for integrating renewable resources into the microgrids. The collaborative nature of such distributed cooperative control-based microgrids can easily spread out a simple cyber-attack on a single DER or a communication link to the entire system, resulting in control failure or even making the overall power system unstable [95–98]. One solution to mitigate such cyber-attacks and maintain the stable operation of microgrids is to develop a resilient controller [8,27,95,99–104]. AI-based techniques are being utilized to design resilient control schemes in microgrids to mitigate the malicious effects of such attacks [42–46,105]. Because of its low computing overhead, effectiveness, and simplicity in design and implementation in a distributed control system, adaptive neuro-fuzzy inference systems (ANFISs) are used for cyber-attack mitigation in an islanded DC microgrid in [42,43]. The proposed framework is based on a residual analysis of the error signal that results from comparing estimated and real detected signals to detect and mitigate the cyber-attack.

NARX ANN is a special class of recurrent neural networks best suited for time series data prediction, input–output modeling of nonlinear dynamical systems, and cyber attack detection in microgrids. Therefore, NARX ANN-based resilient controller is designed to mitigate the cyber-attacks in distributed cooperative control-based AC and DC microgrids in [44,106], respectively.

The proposed controller is trained using the data obtained by simulating the test microgrid system under varying operating conditions. After optimal selection of NARX ANN parameters during offline training, it is deployed as an estimator to generate the reference for the proportional-integral-based controller in [106] whereas, it acts as a secondary level controller to replace the conventional PI-based controller in [44]. Feed-forward ANNs are used to make the existing control resilient in both AC and DC microgrids and showed the improved performance to mitigate the cyber-attacks [46,57,105,107–109]. The proposed technique is based on the reference tracking application for the output DC current of each converter to mitigate the false data. This approach works as a PI-based controller reference tracking application in which the reference is prepared by a Feed-forward ANN that acts as a local estimator for each DER to estimate the output current of the converter. The estimated output from the ANN sets the reference for a PI-based controller whose output is added to the output current of the converter [46,107,108]. This way, the feed-forward ANN maintains the desired reference value in the secondary control layer when false data are injected into the measurements and communication network of the microgrid to mitigate the impact of cyber-attacks. A similar approach utilizing the feed-forward ANN is proposed for a distributed cooperative control-based AC microgrid and a model predictive control-based DC microgrid in [57,109], respectively.

Microgrids are becoming more complex with the increased adoption of electric vehicles, and load frequency control has been effectively utilized to maintain frequency under fluctuating load and generation conditions. For such complex microgrids, a Hyper-basis function neural network is employed to mitigate FDI-type attacks on communication networks and measurements. These attacks may lead the microgrid operation to an unstable state due to incorrect state estimation caused by compromised measurements [45]. In the proposed controller, an intelligent hyper-basis function neural network observer is designed to accurately estimate the state of the microgrids and reconstruct the possible attack signal. Subsequently, a novel hyper-basis ANN-based H_∞ controller is designed to mitigate the negative impact of FDI attacks to maintain the normal operation of the microgrid. In [110], a multi-agent deep reinforcement learning (RL)-based algorithm is proposed for exposing weaknesses in the current cyber-attack detection techniques and laying the groundwork for more dependable cyber-secure solutions, with a focus on DC microgrids. This technique identifies the weak points in the traditional index-based cyber-attack detection schemes and generates coordinated stealthy destabilizing FDI attacks on cyber-secured islanded DC microgrids. A deep deterministic policy gradient is integrated to give trained RL agents a continuous action space and improve the algorithm's accuracy and convergence rate. This method identifies a state-of-the-art detection scheme's sensitivity to a number of coordinated FDI attacks considering the distributed communication delays and load changes. Table 4 provides state-of-the-art AI-based cyber-attack mitigation techniques, their applications in multiple resilient control designs, and a measure of performance metric along with the specific target of cyber-attacks in the microgrids.

Table 4. Summary of AI-based techniques for cyber-attack mitigation in microgrids is provided.

System	Control	Attack	Algorithm	Data	Performance Metric
Islanded DC	Distributed secondary control	FDI into cyber layer	ANFIS	MATLAB simulation, Supervised	Accuracy 99.40%, [42]
	Adaptive model predictive control (APMC)	FDI into voltage and current sensors	ANFIS	MATLAB simulation, Unsupervised	RMSE 0.000846, MAE 0.001543, [43]
	Decentralized cooperative control	FDI into cyber layer (current measurements)	Feed-forward ANN	MATLAB real-time simulation, Supervised	Not given, [46]
	Supervisory control	FDI into secondary control voltage and current measurements	Feed-forward ANN	MATLAB simulation, Supervised	Not given, [105]
	Distributed cooperative secondary control	FDI into cyber layer measurements	Feed-forward ANN	MATLAB real-time simulation, Supervised	Not given, [107]
	Droop control	FDI into output voltage measurements	Deep learning Gated recurrent unit	MATLAB Simulation, Supervised	RMSE <0.05, [80]
	Distributed cooperative secondary control	FDI into cyber layer voltage and current measurements	Feed-forward ANN	MATLAB simulation, Supervised	MSE 5×10^{-10}, [108]
	Distributed cooperative secondary control	FDI into cyber layer current and voltage measurements	NARX ANN	MATLAB simulation, Supervised	Not given, [106]
	Model predictive control	FDI into cyber layer currents and voltages	Feed-forward ANN	MATLAB simulation, Supervised	MSE 2.9×10^{-10}, [109]
	Distributed cooperative secondary control	FDI into cyber layer currents and voltages	Multiagent deep reinforcement learning	MATLAB and dSpace MicroLabBox, Supervised	Not given, [110]
	Synchronous buck converter primary control	FDI into output voltage sensor	Back-propagation ANN	MATLAB simulation, Supervised	RMSE 0.000283, [37]
Islanded AC	Distributed cooperative secondary control	FDI into measurements and communication network	NARX ANN	MATLAB real-time simulation, Supervised	MAPE 0.01%, [44]
	Load frequency control with electric vehicles	FDI into measurements and communication network	Hyper basis function neural network	MATLAB simulation, Supervised	RMSE 0.0015, [45]
	Distributed cooperative secondary control	FDI into measurements and communication network	Feed-forward ANN	MATLAB real-time simulation, Supervised	Not given, [57]
	IEEE distribution networks and islanded microgrid with supervisory control	FDI (Low-frequency source oscillations)	Ensemble learner	Digisilent, Supervised	True positive rate (TPR) >90% False positive rate (FPR) < 3%, [111]

Table 4. *Cont.*

System	Control	Attack	Algorithm	Data	Performance Metric
Islanded AC	Central supervisory control	FDI into smart metering devices and central controller unit	Modified prediction interval-based LSTM	Residential microgrid data, Supervised	Accuracy 97%, [112]
	Secondary control for frequency regulation	DoS and FDI into measurements	Adaptive reinforcement learning	MATLAB real-time simulation, Supervised	MAE 1.2×10^{-5}, [113]

5. Learning-Based Cyber Attack Detection and Mitigation

The vulnerability of microgrids to cyber attacks can be addressed using various data-driven and learning-based techniques for cyber attack detection. The conventional methods are over-reliant on the accurate model of the system while learning-based techniques leverage the computation power and amount of data from the system. Several techniques have been used in the literature to detect and mitigate cyber attacks on microgrids such as transfer learning, explainable learning, ensemble learning, and physics-informed AI.

Transfer learning uses the pre-trained models for the detection of malicious attacks which decreases the need for a huge amount of training data. Transfer learning can be further divided into inductive transfer learning, unsupervised transfer learning, and transducive transfer learning [114]. Representation subspace distance (RSD) based transfer learning is applied to the DNN-based estimator in [115] to improve the cyber security of the microgrid. In smartgrids, cyber-attacks may impede access to local data which can cause issues in power planning and dispatch decisions. Deep transfer learning for load forecasting can provide high-quality load prediction with less data so that in case of missing local data the prediction data are readily available [116]. In general, forecasting methods can be improved by utilizing the generalizing capability of transfer learning without the need for excessive data. A Lower Upper Bound Estimation (LUBE) method is used for FDI attack detection in [117] to provide Prediction intervals (PIs) over smart meter data at the consumer end. In [118], Hilbert–Huang Transform and Deep Learning are employed on distinctive data sets generated via bootstrap for FDI attack detection.

The recent advances in machine learning have improved performance metrics, but the ML models are largely black boxes. Explainable learning or Explainable AI (XAI) is a discipline of AI that tries to explain the predictions and outcomes of machine learning models [119]. From a cyber-security perspective of the microgrid, operators need to trust models and their predictions. XAI is important for the interpretation of decisions in critical scenarios such as flagging a measurement and initiating an inquiry for a particular attack. The cost of misclassification in certain circumstances can be too large [120]. In [121], an XAI framework for fault detection and classification is developed and tested on a 50kW microgrid testbed. An Intrusion Detection System (IDS) is designed in [122] that provides an explanation of each classification through statistics-based measures using Shapley additive explanations (SHAP).

Ensemble learning involves diverse data sets, training various member classifiers, and combining classifier results through various techniques [123]. Extreme-Learning Machines (E^3LM) are used to detect the anomaly cases caused by FDIAs and validated on IEEE 14-, 57-, and 118-bus systems [124]. Physics Informed AI leverages the fusion between the physics-based models and the AI advances. Physics-Informed Neural Networks (PINN) and Physics-Informed Reinforcement Learning find a range of applications in power systems [125–128]. In [129], a Distributed Deep Reinforcement Learning (DRL) strategy is used to design an optimal defensive strategy against FDI attacks in microgrids under a few assumptions. Though promising, the physics-informed AI depends on the accuracy of the model and the dataset. The cyber security of microgrids against attacks can be improved by investing efforts in enhancing the model fidelity. On the other hand, XAI is a relatively new field and it can be leveraged further to make sense of the decisions about the detection of cyber attacks for the grid operators. Various AI-based techniques for cyber-attack detection and mitigation in microgrids are summarized in Figure 5.

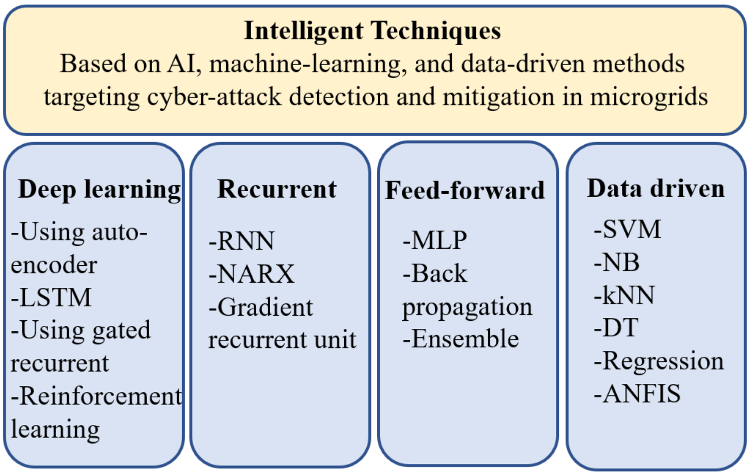


Figure 5. A summary of AI-based cyber-attack detection and mitigation techniques in microgrids is shown.

Table 5 provides a summary of various learning-based techniques for cyber-attack detection and mitigation in microgrids, data acquisition, attack types, and a measure of performance metric.

Table 5. Summary of works using various Learning-based methods for cyber-attack detection and mitigation.

Learning Method	Attack	Algorithm	Data	Performance Metric
Transfer Learning	FDI, DoS	RSD-based transfer learning	MATLAB/Simulink based simulation	RMSE 3.332 × 10^{-3}, [115]
	FDI	Deep transfer learning	Raw power fluctuations data from neighboring cities	MAPE 2.87%, RMSE 0.042, [116]
	FDI	Lower and Upper Bound Estimator (LUBE) combined with Optimization	Smart meters on the customer side	Confusion matrix CR 91.64% FR 8.63%, [117]
	FDI	Deep learning using Krill Herd Optimization algorithm	Distinctive datasets generated via bootstrap	Accuracy 93.76%, [118]
Explainable Learning	FDI	XAI framework using python libraries		Accuracy, recall and precision, [121]
	FDI	Explainable AI using SHAP	UNSW-NB15	True Positive Ration (TPR) and False Positive Ration (FPR), [122]
Physics-based Learning	FDI	DRL	microgrid simulations	Average security level [129]

6. Case Study

To show the effectiveness of AI-based cyber-attack mitigation, an islanded AC microgrid is considered with cyber-attacks targeting the communication network as shown in Figure 6. The physical layer contains DERs and loads, whereas the cyber layer has communication protocols for information exchange among DERs. The primary controller is implemented locally at DERs using a conventional droop control technique that provides a relationship between the frequency ω_i, the reactive power Q_i, the active power P_i, and the voltages v_o.

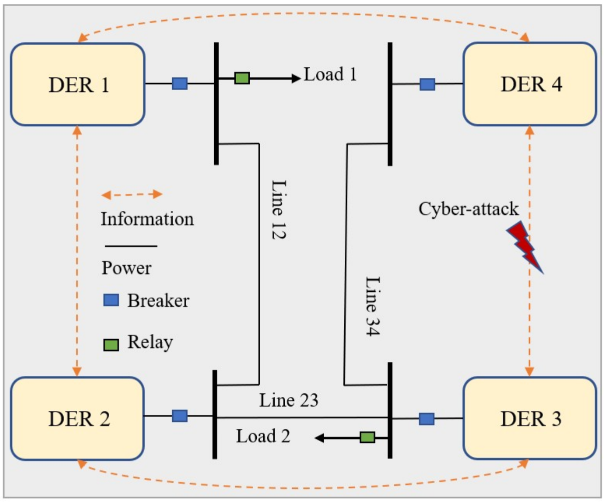


Figure 6. The islanded AC microgrid is implemented with distributed cooperative-based secondary control to manage the four DERs.

The voltage and frequency droop characteristics are given by:

$$\begin{cases} v_o = v^* - n_{Q_i} Q_i, \\ w_i = w^* - m_{P_i} P_i, \end{cases} \tag{3}$$

where v^*, ω^* are the primary voltage and frequency reference values, and m_{P_i}, n_{Q_i} are the active and reactive power droop coefficients, respectively. At the secondary level, distributed cooperative control is utilized to reduce the voltage and frequency error when compared to the nominal values generated by the primary control. The secondary control sets a reference for the primary control such that the voltage and frequency of each DG are synchronized with their respective reference values (v^* and w^*):

$$\begin{cases} \lim_{t\to\infty} \|v_o - v^*\| = 0, \\ \lim_{t\to\infty} \|w_i - w^*\| = 0. \end{cases} \tag{4}$$

The distributed cooperative secondary voltage and frequency control for a single DER requires its own information and that of the neighboring DERs to achieve the control objectives. The reference for the inverters is produced by the voltage and current controllers utilizing droop-control methods [6].

Two types of FDI cyber-attacks are considered for this case study. Firstly, the desired reference set value for the controller is replaced with false data to compel the system to follow an incorrect set of reference values. The attacker replaces the intended signal $u_n(t)$ entirely with its multiple using a constant γ, resulting in:

$$x(u_n(t)) = \begin{cases} u_n(t),\ when\ t < t_o, \\ \gamma * u_n(t),\ when\ t > t_o. \end{cases} \tag{5}$$

FDI cyber-attack is initiated at $t = 2$ s with $\gamma = 0.5$, targeting the DER2 voltage communication link. Secondly, a periodic time-varying cyber-attack is initiated by injecting a periodic sinusoidal signal with time period (ωt) and amplitude ξ into the normal signal u_n, as follows:

$$\psi_n(t) = \begin{cases} 0,\ when\ t < t_o, \\ \xi sin(\omega t) * u_n(t),\ when\ t > t_o. \end{cases} \tag{6}$$

In this case, false data are injected into DER3 voltage communication link at $t = 2$ s with $\xi = 0.5$ and $w = 2\pi 60$ rad/s. The microgrid continues to operate normally for $t < 2$ s.

To mitigate the negative impacts of FDI cyber-attacks a NARX ANN-based resilient controller is designed. to replace the state-of-the-art PI-based controller in the secondary layer of distributed cooperative control. The architecture of NARX ANN has a hidden layer with 10 nodes, an input layer with 13 nodes for voltage and frequency information, and an output layer with four nodes for corresponding reference output for each DER. This structure is optimized after multiple trainings and found best suited for this work. The preceding batch of output and input, $y(k-i)$ and $x(k-i)$, respectively, establish the NARX ANN's output $y(k)$ that constructs an autoregressive model to predict the current value of the dynamical system [44]. These delayed output values act as pseudo-states to extract system dynamics from time series data. This characteristic makes NARX ANN a promising choice for nonlinear dynamical system modeling in applications like intelligent control having a mathematical model given as follows:

$$y(k+1) = f[x(k-n), ..., x(k-d_x-n+1), y(k), ..., y(k-d_y+1)], \tag{7}$$

where $y(k)$ is the model output, $x(k)$ is the model input at discrete time interval k, d_x is input memory order, and d_y is output memory order. AI-based model development involves three main steps including data acquisition, training of the model, and performance evaluation using standard metrics as shown in Figure 7. This model development process is established from the state of the art, and has been effectively implemented in the power systems domain [130].

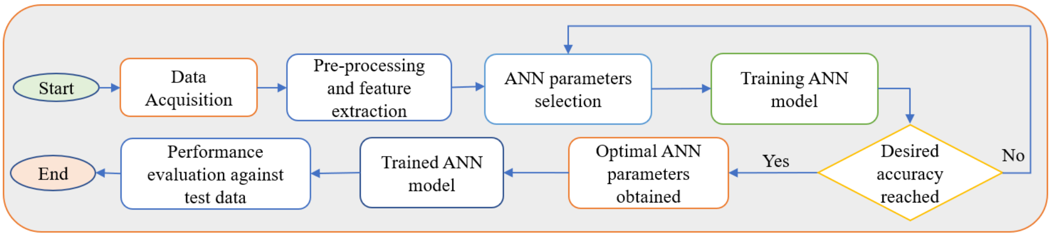


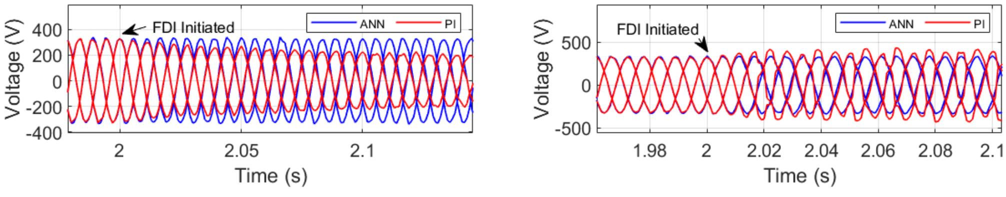
Figure 7. The classical AI-based model development design steps are shown.

The test microgrid in this case study consists of four DERs coupled through RL lines to provide power to two RL loads. This microgrid is designed in MATLAB Simulink with a distributed cooperative control-based secondary controller. The design parameters of the microgrid are given in Table 6. Further details regarding distributed cooperative control design and system parameters can be found in [6,44]. The DERs share voltage and frequency information over the communication network to meet the control objectives.

Table 6. The design parameters of the test microgrid and real-time digital simulator are given.

Parameter	Value	Parameter	Value
L_{12}	(0.23 + j318 µ) Ω	V_{ref}	300 V
L_{23}	(0.35 + j1847 µ) Ω	L_{filter}	1.35 mh
L_{34}	(0.23 + j318 µ) Ω	C_{filter}	50 µF
Simulator	OP5600 from OPAL-RT	Processor	4 Cores, 3.0 GHz
Software	RT-LAB 2019	FPGA	Xilinx® Artix®-7 from OPAL-RT

After the FDI attack, the proposed NARX ANN-based control is compared to the PI-based control, with the results depicted in Figure 8. As illustrated in Figure 8a, the proposed controller maintained the required output voltage at the output of DER2 after the initiation of the FDI cyber-attack. Similarly, after the FDI cyber-attack, the NARX ANN-based voltage controller maintained the specified output voltage at the output of DER3, as shown in Figure 8b. The proposed NARX ANN-based distributed secondary control has demonstrated improved reference tracking capabilities compared to the PI-based control under cyber-attack, as shown in Figure 8.



(**a**) (**b**)

Figure 8. NARX ANN-based controller showed resilient performance in the presence of FDI cyber-attacks compared to the PI-based controller. (**a**) Output voltage of DER2; (**b**) Output voltage of DER3.

7. Discussion

Few AI-based models currently offered in the academic literature have been implemented in practice; the majority are still in the theoretical stage. Many AI and ML approaches, like fuzzy expert, which simulates logical thinking, SVM, which can locate a hyperplane in a high-dimensional space for classifications, and deep learning-based on ANN with numerous hidden layers in the network, have been incorporated into numerous articles. There are multiple reasons for this, such as irreproducible studies, the absence of any benchmarking models or statistics in the literature, and the lack of comparisons to other state-of-the-art models. As a result, the literature is abundant and of diverse quality. In AI-based research studies, models are typically compared with models that are far less capable than the state of the art in that family, rather than with statistical models or other models of AI. Instead of being technique-specific, useful insights and breakthroughs must be transferable between different approaches.

The majority of AI-based modeling uses three stages: initial training to choose parameters, validation to prevent over-fitting, and testing with unknown data that is distinct from the training and validation phases. There are some variations in these stages that are also employed, such as cross-validation, which involves multiple training and validation runs on historical data from various time periods. The selection of parameters is frequently made using metaheuristic algorithms or a mixture of them. Similar to this, several ANNs topologies with varied numbers of neurons, hidden layers, and activation functions are suggested to demonstrate superior performance. Such hyperparameter tuning might be effective in a given situation, but it might not be applicable in all circumstances. Therefore, research needs to shift its emphasis to creating new techniques, useful guidelines, and new ANN structures like recurrent ANN and deep learning with transfer and explainable frameworks. Continuous learning, environment adaptation, and extremely fast output computation are all capabilities of ML approaches. However, addressing the highly intricate nature of power system operations processes to prevent blackouts or to find an optimum operating point without violating any operational limitation is still too safety-critical to accept an ML-based solution. Because there are no performance guarantees, it is challenging for power system operators to trust an AI-based method. AI-based models can be utilized as a tool to help, for instance, by utilizing their computational power to rapidly assess thousands of scenarios. This will aid in the widespread use of AI models in the field of power systems. Applying explainable and interpretable methods is necessary to increase confidence in AI models. This would enable the AI-model output to be verified throughout the whole input space as opposed to just a small dataset. Additionally, physics-informed AI models can be applied by incorporating physics-based models into the training phase of AI models, allowing the model to learn from them rather than creating data as part of the training process.

In order to increase automation, flexibility, and efficiency in operations, energy and critical infrastructure companies are actively developing an industrial Internet of Things (IoT). This is achieved by seamlessly integrating information technology (IT) applications with operational technology (OT) to control physical assets. However, these goals will not be achieved without IoT cybersecurity monitoring and detection. Siemens Energy has developed an AI-based Managed Detection and Response (MDR) system. MDR's monitoring methodology and technology platform leverage AI and machine learning to gather and model energy asset intelligence. Siemens Energy has created a new platform for Security Information and Event Management (SIEM) called *EOS.ii*$^{\mathrm{TM}}$. This is a scalable and adaptable AI-based platform for monitoring and detection and is intended to be the cornerstone of a next-generation fusion security operation center for IoT. It is made to allow for the quick collection, processing, and prioritization of useful information in industrial operating situations. *EOS.ii*$^{\mathrm{TM}}$ applies machine learning to combine IT and OT monitoring and cyber-attack detection capabilities [131,132].

8. Conclusions

This paper provides a comprehensive review of microgrids' cyber vulnerabilities and AI-based techniques to enhance the security of microgrids. This includes AI-based cyber-attack detection and mitigation to achieve a resilient operation of microgrids in the presence of extensive communication networks. Cyber security is addressed from a physical and cyber layer perspective containing power-electronics-based converters, smart metering devices, and information-sharing networks. Cyber-attack's potential targets and their impacts on the operation of microgrids are discussed. AI-based cyber-attack detection and mitigation in microgrids were summarized, along with a case study where utilizing such techniques is presented. In addition, learning-based techniques are also covered to overcome the black-box nature of AI-based models. The proposed ideas have the potential to counter the challenges posed by cyber-attacks on microgrids.

Author Contributions: Conceptualization, O.A.B. and A.A.K.; methodology, O.A.B. and A.A.K.; software, O.A.B. and A.A.K.; validation, O.A.B. and A.A.K.; formal analysis, O.A.B.; investigation, A.A.K.; resources, O.A.B.; data curation, A.A.K., W.U.R. and A.H.; writing—original draft preparation, A.A.K., W.U.R. and A.H.; writing—review and editing, O.A.B. and A.A.K.; visualization, A.A.K.; supervision, O.A.B.; project administration, O.A.B.; funding acquisition, O.A.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

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

References

1. Nassif, A.B.; Ericson, S.; Abbey, C.; Jeffers, R.; Hotchkiss, E.; Bahramirad, S. Valuing Resilience Benefits of Microgrids for an Interconnected Island Distribution System. *Electronics* **2022**, *11*, 4206. [CrossRef]
2. Aghmadi, A.; Hussein, H.; Polara, K.H.; Mohammed, O. A Comprehensive Review of Architecture, Communication, and Cybersecurity in Networked Microgrid Systems. *Inventions* **2023**, *8*, 84. [CrossRef]
3. de la Cruz, J.; Wu, Y.; Candelo-Becerra, J.E.; Vásquez, J.C.; Guerrero, J.M. A review of networked microgrid protection: Architectures, challenges, solutions, and future trends. *CSEE J. Power Energy Syst.* **2023**. . [CrossRef]
4. Bazmohammadi, N.; Madary, A.; Vasquez, J.C.; Mohammadi, H.B.; Khan, B.; Wu, Y.; Guerrero, J.M. Microgrid digital twins: Concepts, applications, and future trends. *IEEE Access* **2021**, *10*, 2284–2302. [CrossRef]
5. Espina, E.; Llanos, J.; Burgos-Mellado, C.; Cardenas-Dobson, R.; Martinez-Gomez, M.; Saez, D. Distributed control strategies for microgrids: An overview. *IEEE Access* **2020**, *8*, 193412–193448. [CrossRef]
6. Nasirian, V.; Moayedi, S.; Davoudi, A.; Lewis, F.L. Distributed cooperative control of DC microgrids. *IEEE Trans. Power Electron.* **2014**, *30*, 2288–2303. [CrossRef]
7. Morstyn, T.; Hredzak, B.; Agelidis, V.G. Distributed cooperative control of microgrid storage. *IEEE Trans. Power Syst.* **2014**, *30*, 2780–2789. [CrossRef]
8. Mustafa, A.; Poudel, B.; Bidram, A.; Modares, H. Detection and mitigation of data manipulation attacks in AC microgrids. *IEEE Trans. Smart Grid* **2019**, *11*, 2588–2603. [CrossRef]
9. Beg, O.A.; Nguyen, L.V.; Johnson, T.T.; Davoudi, A. Signal temporal logic-based attack detection in DC microgrids. *IEEE Trans. Smart Grid* **2018**, *10*, 3585–3595. [CrossRef]
10. Khan, A.A.; Beg, O.A. Cyber Vulnerabilities of Modern Power Systems. In *Power Systems Cybersecurity: Methods, Concepts, and Best Practices*; Haes Alhelou, H., Hatziargyriou, N., Dong, Z.Y., Eds.; Springer International Publishing: Cham, Switzerland, 2023; pp. 47–66. [CrossRef]
11. Bhusal, N.; Abdelmalak, M.; Kamruzzaman, M.; Benidris, M. Power system resilience: Current practices, challenges, and future directions. *IEEE Access* **2020**, *8*, 18064–18086. [CrossRef]

12. Ribas Monteiro, L.F.; Rodrigues, Y.R.; Zambroni de Souza, A. Cybersecurity in Cyber–Physical Power Systems. *Energies* **2023**, *16*, 4556. [CrossRef]
13. Nejabatkhah, F.; Li, Y.W.; Liang, H.; Reza Ahrabi, R. Cyber-security of smart microgrids: A survey. *Energies* **2020**, *14*, 27. [CrossRef]
14. Tan, S.; Wu, Y.; Xie, P.; Guerrero, J.M.; Vasquez, J.C.; Abusorrah, A. New challenges in the design of microgrid systems: Communication networks, cyberattacks, and resilience. *IEEE Electrif. Mag.* **2020**, *8*, 98–106. [CrossRef]
15. Tan, S.; Xie, P.; Guerrero, J.M.; Vasquez, J.C. False data injection cyber-attacks detection for multiple DC microgrid clusters. *Appl. Energy* **2022**, *310*, 118425. [CrossRef]
16. Venkatachary, S.K.; Prasad, J.; Samikannu, R. Cybersecurity and cyber terrorism-in energy sector—A review. *J. Cyber Secur. Technol.* **2018**, *2*, 111–130. [CrossRef]
17. Suprabhath Koduru, S.; Machina, V.S.P.; Madichetty, S. Cyber Attacks in Cyber-Physical Microgrid Systems: A Comprehensive Review. *Energies* **2023**, *16*, 4573. [CrossRef]
18. Krause, T.; Ernst, R.; Klaer, B.; Hacker, I.; Henze, M. Cybersecurity in power grids: Challenges and opportunities. *Sensors* **2021**, *21*, 6225. [CrossRef]
19. MITRE ATT&CK Matrix for Enterprise. Available online: https://attack.mitre.org/ (accessed on 10 November 2023).
20. Ramotsoela, D.T.; Hancke, G.P.; Abu-Mahfouz, A.M. Practical Challenges of Attack Detection in Microgrids Using Machine Learning. *J. Sens. Actuator Netw.* **2023**, *12*, 7. [CrossRef]
21. Karanfil, M.; Rebbah, D.E.; Debbabi, M.; Kassouf, M.; Ghafouri, M.; Youssef, E.N.S.; Hanna, A. Detection of Microgrid Cyberattacks Using Network and System Management. *IEEE Trans. Smart Grid* **2023**, *14*, 2390–2405. [CrossRef]
22. Pinto, S.J.; Siano, P.; Parente, M. Review of Cybersecurity Analysis in Smart Distribution Systems and Future Directions for Using Unsupervised Learning Methods for Cyber Detection. *Energies* **2023**, *16*, 1651. [CrossRef]
23. Ortega-Fernandez, I.; Liberati, F. A Review of Denial of Service Attack and Mitigation in the Smart Grid Using Reinforcement Learning. *Energies* **2023**, *16*, 635. [CrossRef]
24. Kim, Y.; Hakak, S.; Ghorbani, A. Smart grid security: Attacks and defence techniques. *IET Smart Grid* **2023**, *6*, 103–123. [CrossRef]
25. Sahoo, S.; Blaabjerg, F.; Dragicevic, T. (Eds.) *Cyber Security for Microgrids*; IEEE: New York, NY, USA, 2022. [CrossRef]
26. Leng, M.; Sahoo, S.; Blaabjerg, F.; Molinas, M. Projections of Cyberattacks on Stability of DC Microgrids—Modeling Principles and Solution. *IEEE Trans. Power Electron.* **2022**, *37*, 11774–11786. [CrossRef]
27. Jamali, M.; Sadabadi, M.S.; Davari, M.; Sahoo, S.; Blaabjerg, F. Resilient Cooperative Secondary Control of Islanded AC Microgrids Utilizing Inverter-Based Resources Against State-Dependent False Data Injection Attacks. *IEEE Trans. Power Electron.* **2023**, 1–12. . [CrossRef]
28. Abdullahi, M.; Baashar, Y.; Alhussian, H.; Alwadain, A.; Aziz, N.; Capretz, L.F.; Abdulkadir, S.J. Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. *Electronics* **2022**, *11*, 198. [CrossRef]
29. Trivedi, R.; Khadem, S. Implementation of artificial intelligence techniques in microgrid control environment: Current progress and future scopes. *Energy AI* **2022**, *8*, 100147. [CrossRef]
30. Nair, D.R.; Nair, M.G.; Thakur, T. A smart microgrid system with artificial intelligence for power-sharing and power quality improvement. *Energies* **2022**, *15*, 5409. [CrossRef]
31. Wu, T.; Wang, J. Artificial intelligence for operation and control: The case of microgrids. *Electr. J.* **2021**, *34*, 106890. [CrossRef]
32. Lv, L.; Wu, Z.; Zhang, L.; Gupta, B.B.; Tian, Z. An Edge-AI Based Forecasting Approach for Improving Smart Microgrid Efficiency. *IEEE Trans. Ind. Inform.* **2022**, *18*, 7946–7954. [CrossRef]
33. Zhao, S.; Blaabjerg, F.; Wang, H. An Overview of Artificial Intelligence Applications for Power Electronics. *IEEE Trans. Power Electron.* **2021**, *36*, 4633–4658. [CrossRef]
34. Dewangan, F.; Abdelaziz, A.Y.; Biswal, M. Load Forecasting Models in Smart Grid Using Smart Meter Information: A Review. *Energies* **2023**, *16*, 1404. [CrossRef]
35. Poti, K.D.; Naidoo, R.M.; Mbungu, N.T.; Bansal, R.C. Intelligent solar photovoltaic power forecasting. *Energy Rep.* **2023**, *9*, 343–352. [CrossRef]
36. Yang, Y.; Guo, L.; Li, X.; Li, J.; Liu, W.; He, H. A data-driven detection strategy of false data in cooperative DC microgrids. In Proceedings of the IECON 2021—47th Annual Conference of the IEEE Industrial Electronics Society, Toronto, ON, Canada, 13–16 October 2021; pp. 1–6.
37. Banda, M.K.; Koduru, S.S.; Machina, V.S.P.; Madichetty, S. A Deep Learning Based Cyber Attack Detection and Mitigation Scheme in Synchronous Buck Converter. In Proceedings of the 2022 IEEE International Conference on Power Electronics, Drives and Energy Systems (PEDES), Jaipur, India, 14–17 December 2022; pp. 1–6.
38. Suprabhath, K.; Prasad, M.V.S.; Chetty, S.; Mishra, S. A deep learning based cyber attack detection scheme in DC microgrid systems. *CPSS Trans. Power Electron. Appl.* **2023**, *8*, 2. [CrossRef]
39. Siniosoglou, I.; Radoglou-Grammatikis, P.; Efstathopoulos, G.; Fouliras, P.; Sarigiannidis, P. A unified deep learning anomaly detection and classification approach for smart grid environments. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 1137–1151. [CrossRef]
40. Panthi, M. Anomaly detection in smart grids using machine learning techniques. In Proceedings of the 2020 First International Conference on Power, Control and Computing Technologies (ICPC2T), Raipur, India, 3–5 January 2020; pp. 220–222.
41. Glauner, P. Big Data-Driven Detection of False Data Injection Attacks in Smart Meters. *IEEE Access* **2021**, *9*, 144313–144326.

42. Basati, A.; Guerrero, J.M.; Vasquez, J.C.; Bazmohammadi, N.; Golestan, S. A Data-Driven Framework for FDI Attack Detection and Mitigation in DC Microgrids. *Energies* **2022**, *15*, 8539. [CrossRef]
43. Abazari, A.; Zadsar, M.; Ghafouri, M.; Atallah, R.; Assi, C. A data mining/anfis and adaptive control for detection and mitigation of attacks on dc mgs. *IEEE Trans. Smart Grid* **2022**, *14*, 2406–2422. [CrossRef]
44. Khan, A.A.; Beg, O.A.; Jin, Y.F.; Ahmed, S. An Explainable Intelligent Framework for Anomaly Mitigation in Cyber-Physical Inverter-based Systems. *IEEE Access* **2023**, *11*, 65382–65394. [CrossRef]
45. Tian, E.; Wu, Z.; Xie, X. Codesign of FDI Attacks Detection, Isolation, and Mitigation for Complex Microgrid Systems: An HBF-NN-Based Approach. *IEEE Trans. Neural Netw. Learn. Syst.* **2022**. . [CrossRef]
46. Habibi, M.R.; Sahoo, S.; Rivera, S.; Dragičević, T.; Blaabjerg, F. Decentralized coordinated cyberattack detection and mitigation strategy in DC microgrids based on artificial neural networks. *IEEE J. Emerg. Sel. Top. Power Electron.* **2021**, *9*, 4629–4638. [CrossRef]
47. Zhang, N.; Sun, Q.; Yang, L.; Li, Y. Event-Triggered Distributed Hybrid Control Scheme for the Integrated Energy System. *IEEE Trans. Ind. Inform.* **2022**, *18*, 835–846. [CrossRef]
48. Yang, L.; Li, X.; Sun, M.; Sun, C. Hybrid Policy-Based Reinforcement Learning of Adaptive Energy Management for the Energy Transmission-Constrained Island Group. *IEEE Trans. Ind. Inform.* **2023**, *19*, 10751–10762. [CrossRef]
49. AlSkaif, T.; Crespo-Vazquez, J.L.; Sekuloski, M.; van Leeuwen, G.; Catalão, J.P.S. Blockchain-Based Fully Peer-to-Peer Energy Trading Strategies for Residential Energy Systems. *IEEE Trans. Ind. Inform.* **2022**, *18*, 231–241. [CrossRef]
50. Cui, S.; Wang, Y.W.; Shi, Y.; Xiao, J.W. A new and fair peer-to-peer energy sharing framework for energy buildings. *IEEE Trans. Smart Grid* **2020**, *11*, 3817–3826. [CrossRef]
51. Lopez-Garcia, T.B.; Coronado-Mendoza, A.; Domínguez-Navarro, J.A. Artificial neural networks in microgrids: A review. *Eng. Appl. Artif. Intell.* **2020**, *95*, 103894. [CrossRef]
52. Singh, N.K.; Mahajan, V. Analysis and evaluation of cyber-attack impact on critical power system infrastructure. *Smart Sci.* **2021**, *9*, 1–13. [CrossRef]
53. Pour, M.M.; Anzalchi, A.; Sarwat, A. A review on cyber security issues and mitigation methods in smart grid systems. In Proceedings of the SoutheastCon 2017, Concord, NC, USA, 30 March–2 April 2017; pp. 1–4.
54. Reda, H.T.; Anwar, A.; Mahmood, A. Comprehensive survey and taxonomies of false data injection attacks in smart grids: Attack models, targets, and impacts. *Renew. Sustain. Energy Rev.* **2022**, *163*, 112423. [CrossRef]
55. Olowu, T.O.; Dharmasena, S.; Hernandez, A.; Sarwat, A. Impact analysis of cyber attacks on smart grid: A review and case study. In *New Research Directions in Solar Energy Technologies*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 31–51.
56. Liang, G.; Zhao, J.; Luo, F.; Weller, S.R.; Dong, Z.Y. A review of false data injection attacks against modern power systems. *IEEE Trans. Smart Grid* **2016**, *8*, 1630–1638. [CrossRef]
57. Khan, A.A.; Beg, O.A.; Alamaniotis, M.; Ahmed, S. Intelligent anomaly identification in cyber-physical inverter-based systems. *Electric Power Syst. Res.* **2021**, *193*, 107024. [CrossRef]
58. Peng, C.; Sun, H.; Yang, M.; Wang, Y.L. A survey on security communication and control for smart grids under malicious cyber attacks. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 1554–1569. [CrossRef]
59. Zhang, H.; Liu, B.; Wu, H. Smart grid cyber-physical attack and defense: A review. *IEEE Access* **2021**, *9*, 29641–29659. [CrossRef]
60. Huseinović, A.; Mrdović, S.; Bicakci, K.; Uludag, S. A survey of denial-of-service attacks and solutions in the smart grid. *IEEE Access* **2020**, *8*, 177447–177470. [CrossRef]
61. Li, F.; Yan, X.; Xie, Y.; Sang, Z.; Yuan, X. A review of cyber-attack methods in cyber-physical power system. In Proceedings of the 2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP), Xi'an, China, 21–24 October 2019; pp. 1335–1339.
62. Wlazlo, P.; Sahu, A.; Mao, Z.; Huang, H.; Goulart, A.; Davis, K.; Zonouz, S. Man-in-the-middle attacks and defence in a power system cyber-physical testbed. *IET Cyber-Phys. Syst. Theory Appl.* **2021**, *6*, 164–177. [CrossRef]
63. Das, A.K.; Zeadally, S. Data security in the smart grid environment. In *Pathways to a Smarter Power System*; Elsevier: Amsterdam, The Netherlands, 2019; pp. 371–395.
64. Zhang, Z.; Ning, H.; Shi, F.; Farha, F.; Xu, Y.; Xu, J.; Zhang, F.; Choo, K.K.R. Artificial intelligence in cyber security: Research advances, challenges, and opportunities. *Artif. Intell. Rev.* **2022**, *55*, 1029–1053. [CrossRef]
65. Zhang, Y.; Liu, J.; Shen, W. A Review of Ensemble Learning Algorithms Used in Remote Sensing Applications. *Appl. Sci.* **2022**, *12*, 8654. [CrossRef]
66. Mienye, I.D.; Sun, Y. A Survey of Ensemble Learning: Concepts, Algorithms, Applications, and Prospects. *IEEE Access* **2022**, *10*, 99129–99149. [CrossRef]
67. Harrou, F.; Taghezouit, B.; Khadraoui, S.; Dairi, A.; Sun, Y.; Hadj Arab, A. Ensemble Learning Techniques-Based Monitoring Charts for Fault Detection in Photovoltaic Systems. *Energies* **2022**, *15*, 6716. [CrossRef]
68. Arman, A.; Krishnan, V.V.G.; Srivastava, A.; Wu, Y.; Sindhu, S. Cyber physical security analytics for transactive energy systems using ensemble machine learning. In Proceedings of the 2018 North American Power Symposium (NAPS), Fargo, ND, USA, 9–11 September 2018; pp. 1–6. [CrossRef]
69. Goyel, H.; Swarup, K.S. Data Integrity Attack Detection Using Ensemble-Based Learning for Cyber–Physical Power Systems. *IEEE Trans. Smart Grid* **2023**, *14*, 1198–1209. [CrossRef]

70. Liu, S.; You, S.; Yin, H.; Lin, Z.; Liu, Y.; Yao, W.; Sundaresh, L. Model-Free Data Authentication for Cyber Security in Power Systems. *IEEE Trans. Smart Grid* **2020**, *11*, 4565–4568. [CrossRef]
71. Toker, O.; Khalghani, M.R. Cyber Anomaly Detection Design for Microgrids using an Artificial Intelligent-Based Method. In Proceedings of the 2022 North American Power Symposium (NAPS), Salt Lake City, UT, USA, 9–11 October 2022; pp. 1–5. [CrossRef]
72. Dehghani, M.; Niknam, T.; Ghiasi, M.; Bayati, N.; Savaghebi, M. Cyber-Attack Detection in DC Microgrids Based on Deep Machine Learning and Wavelet Singular Values Approach. *Electronics* **2021**, *10*, 1914. [CrossRef]
73. Dehghani, M.; Kavousi-Fard, A.; Dabbaghjamanesh, M.; Avatefipour, O. Deep learning based method for false data injection attack detection in AC smart islands. *IET Gener. Transm. Distrib.* **2020**, *14*, 5756–5765. [CrossRef]
74. Mao, J. Data-Driven Cyberattack Detection for Microgrids. Master's Thesis, KTH School of Electrical Engineering and Computer Science, Stockholm, Sweden, 2022.
75. Reda, H.T.; Anwar, A.; Mahmood, A.; Chilamkurti, N. Data-driven approach for state prediction and detection of false data injection attacks in smart grid. *J. Mod. Power Syst. Clean Energy* **2022**, *11*, 455–467. [CrossRef]
76. Habibi, M.R.; Baghaee, H.R.; Dragičević, T.; Blaabjerg, F. Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks. *IEEE J. Emerg. Sel. Top. Power Electron.* **2020**, *9*, 5294–5310. [CrossRef]
77. Kwon, S.; Yoo, H.; Shon, T. IEEE 1815.1-based power system security with bidirectional RNN-based network anomalous attack detection for cyber-physical system. *IEEE Access* **2020**, *8*, 77572–77586. [CrossRef]
78. Qiu, W.; Tang, Q.; Wang, Y.; Zhan, L.; Liu, Y.; Yao, W. Multi-view convolutional neural network for data spoofing cyber-attack detection in distribution synchrophasors. *IEEE Trans. Smart Grid* **2020**, *11*, 3457–3468. [CrossRef]
79. Naderi, E.; Asrari, A. Toward detecting cyberattacks targeting modern power grids: A deep learning framework. In Proceedings of the 2022 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, 6–9 June 2022; pp. 357–363.
80. He, Q.; Shah, P.; Zhao, X. Resilient operation of DC microgrid against FDI attack: A GRU based framework. *Int. J. Electr. Power Energy Syst.* **2023**, *145*, 108586. [CrossRef]
81. Wan, Y.; Dragičević, T. Data-driven cyber-attack detection of intelligent attacks in islanded dc microgrids. *IEEE Trans. Power Electron.* **2022**, *70*, 4293–4299. [CrossRef]
82. Sourav, S.; Biswas, P.P.; Chen, B.; Mashima, D. Detecting Hidden Attackers in Photovoltaic Systems Using Machine Learning. In Proceedings of the 2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Singapore, 25–28 October 2022; pp. 360–366.
83. Li, F.; Xie, R.; Yang, B.; Guo, L.; Ma, P.; Shi, J.; Ye, J.; Song, W. Detection and identification of cyber and physical attacks on distribution power grids with pvs: An online high-dimensional data-driven approach. *IEEE J. Emerg. Sel. Top. Power Electron.* **2019**, *10*, 1282–1291. [CrossRef] [PubMed]
84. Hakim, M.S.S.; Karegar, H.K. Detection of False Data Injection Attacks Using Cross Wavelet Transform and Machine Learning. In Proceedings of the 2021 11th Smart Grid Conference (SGC), Tabriz, Iran, 7–9 December 2021; pp. 1–5.
85. Qiu, W.; Tang, Q.; Zhu, K.; Yao, W.; Ma, J.; Liu, Y. Cyber spoofing detection for grid distributed synchrophasor using dynamic dual-kernel SVM. *IEEE Trans. Smart Grid* **2020**, *12*, 2732–2735. [CrossRef]
86. Ahmed, S.; Lee, Y.; Hyun, S.H.; Koo, I. Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2765–2777. [CrossRef]
87. Zhang, Y.; Yan, J. Domain-adversarial transfer learning for robust intrusion detection in the smart grid. In Proceedings of the 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Beijing, China, 21–23 October 2019; pp. 1–6.
88. EL-Ebiary, A.H.; Mokhtar, M.; Mansour, A.M.; Awad, F.H.; Marei, M.I.; Attia, M.A. Distributed Mitigation Layers for Voltages and Currents Cyber-Attacks on DC Microgrids Interfacing Converters. *Energies* **2022**, *15*, 9426. [CrossRef]
89. Naderi, E.; Asrari, A. Detection of False Data Injection Cyberattacks: Experimental Validation on a Lab-scale Microgrid. In Proceedings of the 2022 IEEE Green Energy and Smart System Systems (IGESSC), Long Beach, CA, USA, 7–8 November 2022; pp. 1–6.
90. Canaan, B.; Colicchio, B.; Abdeslam, D.O. Experimental HIl implementation of RNN for detecting cyber physical attacks in AC microgrids. In Proceedings of the 2022 International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM), Sorrento, Italy, 22–24 June 2022; pp. 958–963.
91. Mohiuddin, S.M.; Qi, J.; Fung, S.; Huang, Y.; Tang, Y. Deep learning based multi-label attack detection for distributed control of AC microgrids. In Proceedings of the 2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Aachen, Germany, 25–28 October 2021; pp. 233–238 .
92. Canaan, B.; Colicchio, B.; Abdeslam, D.O.; Idoumghar, L. LSTM Networks for Cyber-physical Attack Diagnoses in Microgrids. In Proceedings of the 2023 IEEE 32nd International Symposium on Industrial Electronics (ISIE), Helsinki, Finland, 19–21 June 2023; pp. 1–6.
93. Jadidi, S.; Badihi, H.; Zhang, Y. Design of an intelligent hybrid diagnosis scheme for cyber-physical PV systems at the microgrid level. *Int. J. Electr. Power Energy Syst.* **2023**, *150*, 109062. [CrossRef]
94. Warraich, Z.; Morsi, W. Early detection of cyber–physical attacks on fast charging stations using machine learning considering vehicle-to-grid operation in microgrids. *Sustain. Energy Grids Netw.* **2023**, *34*, 101027. [CrossRef]

95. Chen, Y.; Qi, D.; Dong, H.; Li, C.; Li, Z.; Zhang, J. A FDI attack-resilient distributed secondary control strategy for islanded microgrids. *IEEE Trans. Smart Grid* **2020**, *12*, 1929–1938. [CrossRef]
96. Ye, J.; Giani, A.; Elasser, A.; Mazumder, S.K.; Farnell, C.; Mantooth, H.A.; Kim, T.; Liu, J.; Chen, B.; Seo, G.S.; et al. A review of cyber–physical security for photovoltaic systems. *IEEE J. Emerg. Sel. Top. Power Electron.* **2021**, *10*, 4879–4901. [CrossRef]
97. Gaggero, G.B.; Girdinio, P.; Marchese, M. Advancements and research trends in microgrids cybersecurity. *Appl. Sci.* **2021**, *11*, 7363. [CrossRef]
98. Rana, M.M.; Li, L.; Su, S.W. Cyber attack protection and control of microgrids. *IEEE/CAA J. Autom. Sin.* **2017**, *5*, 602–609. [CrossRef]
99. Sahoo, S.; Yang, Y.; Blaabjerg, F. Resilient synchronization strategy for AC microgrids under cyber attacks. *IEEE Trans. Power Electron.* **2020**, *36*, 73–77. [CrossRef]
100. Sahoo, S.; Dragičević, T.; Blaabjerg, F. Multilayer resilience paradigm against cyber attacks in DC microgrids. *IEEE Trans. Power Electron.* **2020**, *36*, 2522–2532. [CrossRef]
101. Zhang, J.; Sahoo, S.; Peng, J.C.H.; Blaabjerg, F. Mitigating concurrent false data injection attacks in cooperative dc microgrids. *IEEE Trans. Power Electron.* **2021**, *36*, 9637–9647. [CrossRef]
102. Mishra, S.; Anderson, K.; Miller, B.; Boyer, K.; Warren, A. Microgrid resilience: A holistic approach for assessing threats, identifying vulnerabilities, and designing corresponding mitigation strategies. *Appl. Energy* **2020**, *264*, 114726. [CrossRef]
103. Naderi, E.; Asrari, A. Experimental Validation of a Remedial Action via Hardware-in-the-loop System Against Cyberattacks Targeting a Lab-scale PV/Wind Microgrid. *IEEE Trans. Smart Grid* **2023**, *14*, 4060–4072. [CrossRef]
104. Danilczyk, W.; Sun, Y.; He, H. ANGEL: An intelligent digital twin framework for microgrid security. In Proceedings of the 2019 North American Power Symposium (NAPS), Wichita, KS, USA, 13–15 October 2019; pp. 1–6.
105. Zeng, H.; Zhao, Y.; Wang, T.; Zhang, J. Defense Strategy against False Data Injection Attacks in Ship DC Microgrids. *J. Mar. Sci. Eng.* **2022**, *10*, 1930. [CrossRef]
106. Habibi, M.R.; Dragicevic, T.; Blaabjerg, F. Secure control of dc microgrids under cyber-attacks based on recurrent neural networks. In Proceedings of the 2020 IEEE 11th International Symposium on Power Electronics for Distributed Generation Systems (PEDG), Dubrovnik, Croatia, 28 September–1 October 2020; pp. 517–521.
107. Habibi, M.R.; Baghaee, H.R.; Dragičević, T.; Blaabjerg, F. False data injection cyber-attacks mitigation in parallel DC/DC converters based on artificial neural networks. *IEEE Trans. Circuits Syst. II Express Briefs* **2020**, *68*, 717–721. [CrossRef]
108. Habibi, M.R.; Baghaee, H.R.; Blaabjerg, F.; Dragičević, T. Secure control of DC microgrids for instant detection and mitigation of cyber-attacks based on artificial intelligence. *IEEE Syst. J.* **2021**, *16*, 2580–2591. [CrossRef]
109. Habibi, M.R.; Baghaee, H.R.; Blaabjerg, F.; Dragičević, T. Secure MPC/ANN-based false data injection cyber-attack detection and mitigation in DC microgrids. *IEEE Syst. J.* **2021**, *16*, 1487–1498. [CrossRef]
110. Abianeh, A.J.; Wan, Y.; Ferdowsi, F.; Mijatovic, N.; Dragičević, T. Vulnerability identification and remediation of fdi attacks in islanded dc microgrids using multiagent reinforcement learning. *IEEE Trans. Power Electron.* **2021**, *37*, 6359–6370. [CrossRef]
111. Basati, A.; Bazmohammadi, N.; Guerrero, J.M.; Vasquez, J.C. Real-time estimation in cyber attack detection and mitigation framework for dc microgrids. In Proceedings of the 2023 23rd International Scientific Conference on Electric Power Engineering (EPE), Brno, Czech Republic, 24–26 May 2023; pp. 1–6.
112. Ye, Z.; Yang, H.; Zheng, M. Using modified prediction interval-based machine learning model to mitigate data attack in microgrid. *Int. J. Electr. Power Energy Syst.* **2021**, *129*, 106847. [CrossRef]
113. Heidary, J.; Oshnoei, S.; Gheisarnejad, M.; Khalghani, M.R.; Khooban, M.H. Shipboard Microgrid Frequency Control Based on Machine Learning Under Hybrid Cyberattacks. *IEEE Trans. Power Electron.* **2023**. . [CrossRef]
114. Alhelou, H.H.; Hatziargyriou, N.; Dong, Z.Y. *Power Systems Cybersecurity: Methods, Concepts, and Best Practices*; Springer Nature: Berlin/Heidelberg, Germany, 2023.
115. Xia, Y.; Xu, Y.; Mondal, S.; Gupta, A.K. A Transfer Learning-Based Method for Cyber-Attack Tolerance in Distributed Control of Microgrids. *IEEE Trans. Smart Grid* **2023**. . [CrossRef]
116. Zhao, L.; Zhang, X.; Chen, Y.; Peng, X.; Cao, Y. An Improved Load Forecasting Method Based on the Transfer Learning Structure under Cyber-Threat Condition. *Comput. Intell. Neurosci.* **2022**, *2022*, 1696663. [CrossRef] [PubMed]
117. Kavousi-Fard, A.; Su, W.; Jin, T. A machine-learning-based cyber attack detection model for wireless sensor networks in microgrids. *IEEE Trans. Ind. Inform.* **2020**, *17*, 650–658. [CrossRef]
118. Cui, H.; Dong, X.; Deng, H.; Dehghani, M.; Alsubhi, K.; Aljahdali, H.M.A. Cyber attack detection process in sensor of DC micro-grids under electric vehicle based on Hilbert–Huang transform and deep learning. *IEEE Sensors J.* **2020**, *21*, 15885–15894. [CrossRef]
119. Javed, A.R.; Ahmed, W.; Pandya, S.; Maddikunta, P.K.R.; Alazab, M.; Gadekallu, T.R. A survey of explainable artificial intelligence for smart cities. *Electronics* **2023**, *12*, 1020. [CrossRef]
120. Machlev, R.; Heistrene, L.; Perl, M.; Levy, K.; Belikov, J.; Mannor, S.; Levron, Y. Explainable Artificial Intelligence (XAI) techniques for energy and power systems: Review, challenges and opportunities. *Energy AI* **2022**, *9*, 100169. [CrossRef]
121. Ajayi, O. Explainable AI (XAI) for Fault Detection and Classification in Microgrids Using a Real-Time Simulation Framework. Master's Thesis, The Pennsylvania State University, State College, PA, USA, 2023.
122. Larriva-Novo, X.; Sánchez-Zas, C.; Villagrá, V.A.; Marín-Lopez, A.; Berrocal, J. Leveraging Explainable Artificial Intelligence in Real-Time Cyberattack Identification: Intrusion Detection System Approach. *Appl. Sci.* **2023**, *13*, 8587. [CrossRef]

123. Zhang, C.; Ma, Y. *Ensemble Machine Learning: Methods and Applications*; Springer: Berlin/Heidelberg, Germany, 2012.
124. Wu, T.; Xue, W.; Wang, H.; Chung, C.; Wang, G.; Peng, J.; Yang, Q. Extreme learning machine-based state reconstruction for automatic attack filtering in cyber physical power system. *IEEE Trans. Ind. Inform.* **2020**, *17*, 1892–1904. [CrossRef]
125. Huang, B.; Wang, J. Applications of physics-informed neural networks in power systems—A review. *IEEE Trans. Power Syst.* **2022**, *38*, 572–588. [CrossRef]
126. She, B.; Li, F.; Cui, H.; Shuai, H.; Oboreh-Snapps, O.; Bo, R.; Praisuwanna, N.; Wang, J.; Tolbert, L.M. Inverter PQ Control with Trajectory Tracking Capability for Microgrids Based on Physics-informed Reinforcement Learning. *IEEE Trans. Smart Grid* **2023**. . [CrossRef]
127. Wang, L.; Zhang, S.; Zhou, Y.; Fan, C.; Zhang, P.; Shamash, Y.A. Physics-Informed, Safety and Stability Certified Neural Control for Uncertain Networked Microgrids. *IEEE Trans. Smart Grid* **2023**. . [CrossRef]
128. Wang, Y.; Qiu, D.; Sun, M.; Strbac, G.; Gao, Z. Secure energy management of multi-energy microgrid: A physical-informed safe reinforcement learning approach. *Appl. Energy* **2023**, *335*, 120759. [CrossRef]
129. Zhang, H.; Yue, D.; Dou, C.; Hancke, G.P. Resilient optimal defensive strategy of micro-grids system via distributed deep reinforcement learning approach against fdi attack. *IEEE Trans. Neural Netw. Learn. Syst.* **2022**. . [CrossRef] [PubMed]
130. Chatzivasileiadis, S.; Venzke, A.; Stiasny, J.; Misyris, G. Machine learning in power systems: Is it time to trust it? *IEEE Power Energy Mag.* **2022**, *20*, 32–41. [CrossRef]
131. Simonovich, L. Leveraging Security Analytics To Mitigate the Risk of Cyberattacks on Oil & Gas Infrastructure. In Proceedings of the World Petroleum Congress, WPC, Moscow, Russia, 15–19 June 2014; p. D021S019R003.
132. SiemensEnergy. Industrial Cybersecurity *EOS.ii*$^{\text{TM}}$ Monitoring and Detection Platform. Available online: https://assets.siemens-energy.com/siemens/assets/api/uuid:c7ac7495-74a5-482f-81c7-fac6b45e5689/EOS.ii-Whitepaper-21-09-14.pdf (accessed on 10 November 2023).

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