Received 13 August 2023; revised 25 December 2023; accepted 8 February 2024. Date of publication 13 February 2024; date of current version 29 February 2024. The review of this article was arranged by Associate Editor X. Liang.

Digital Object Identifier 10.1109/OJIA.2024.3365576

Command Injection Attacks in Smart Grids: A Survey

MUHAMMAD USAMA AND MUHAMMAD NAVEED AMAN (Senior Member, IEEE)

School of Computing, University of Nebraska–Lincoln, Lincoln, NE 68588 USA

CORRESPONDING AUTHOR: MUHAMMAD NAVEED AMAN. (Email: naveed.aman@unl.edu)

ABSTRACT Cybersecurity is important in the realization of various smart grid technologies. Several studies have been conducted to discuss different types of cyberattacks and provide their countermeasures. The false command injection attack (FCIA) is considered one of the most critical attacks that have been studied. Various techniques have been proposed in the literature to detect FCIAs on different components of smart grids. The predominant focus of current surveys lies on FCIAs and detection techniques for such attacks. This article presents a survey of existing works on FCIAs and classifies FCIAs in smart grids according to the targeted component. The impacts of FCIAs on smart grids are also discussed. Subsequently, this article provides an extensive review of detection studies, categorizing them based on the type of detection technique employed.

INDEX TERMS Artificial intelligence (AI)-based detection algorithms, command injection, cyber-physical systems (CPSs), detection techniques, model-based detection, smart grid.

I. INTRODUCTION

The smart grid is an advanced electrical power system that integrates modern communications and information technologies to optimize the generation, distribution, and consumption of electricity. Integration of smart grid technology into the power industry has revolutionized the way we generate, transmit, and consume energy. Increasing adoption of smart grids has brought about numerous benefits for the power sector, such as improved efficiency, reliability, connectivity, and integration of renewable energy sources [1]. Smart grid technology has additional benefits such as improved demand response, cost savings, better customer involvement, lower CO_2 emissions, and integration of renewable energy technologies and electric vehicles [2], [3]. The electricity grid is an ideal illustration of a cyber-physical system (CPS) due to its integration of information and communication technology [4]. Now that they are linked to the Internet, critical smart grid components, including distribution management systems and advanced metering infrastructure, are open to cyberattacks. This raises questions about the capacity to safeguard private information and guarantee power supply continuity. Hence, a number of research studies have been conducted to study and improve the security aspects of smart grids [5], [6]. These studies focus on identifying potential vulnerabilities and proposing effective and dependable solutions, whether on the cyber or physical level. These efforts have been undertaken in response to the increasing threat of CPS attacks on smart grids and their applications [7].

In 2013, the Presidential Policy Directive 21 (PPD-21) that provided a consistent strategy for the protection of critical infrastructure across the United States was released [8]. Sixteen critical infrastructure sectors were identified by the PPD-21 as being crucial to the safety, well-being, and economic vitality of the nation. Each of these 16 critical infrastructure sectors has been identified based on the level of impact their failure would have on national security, public health and safety, and economic prosperity. The PPD-21 also establishes a framework for the identification, assessment, prioritization, and protection of critical infrastructure. As shown in Fig. 1, the PPD-21 includes the energy sector as one of the 16 critical infrastructure sectors and recognizes the importance of maintaining a reliable and secure energy supply to support all other critical infrastructure sectors [9].

The energy sector constitutes the foundational infrastructure supporting a nation's economic activities. The potential losses from a 6-h blackout in France that could exceed

© 2024 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License. For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

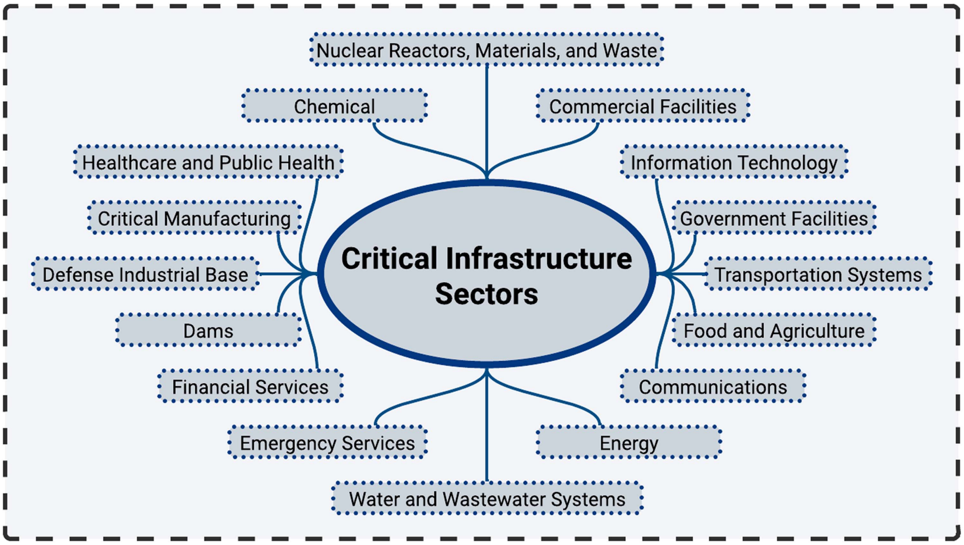

FIGURE 1. Critical infrastructure sectors identified by the PPD-21 [8].

EUR 1.5 billion serve as an illustration of this [10]. Moreover, the energy sector heavily depends on distributed and complex infrastructure, thereby presenting a larger attack surface for malicious threat actors. In addition, the energy sector is perceived as a late adopter of digital transformation, indicating an inherent deficiency in cybersecurity expertise and maturity. This makes the energy sector an appealing target for cyberattacks apparent from several cyberattacks in the energy industry in recent years [11]. These attacks have varied in their impact, with some causing minimal disruption and others resulting in explosions, significant financial loss, and even loss of human lives. The increasing frequency of these incidents is a major concern. For instance, the U.S. Energy Department recorded 362 instances of power outages linked to CPS assaults between 2011 and 2014 [12]. A 2017 report [13] found that 54% of the organizations surveyed reported having dealt with a CPS security issue in the previous year and 21% reported dealing with two or more issues at the same time. Governments from all around the world have responded to these occurrences by issuing guidelines for safeguarding smart grids by the National Institute of Standards and Technology (NIST) and the U.S. Executive Order 13636 to improve cybersecurity in vital infrastructure [14]. As a result, scientists are currently striving to comprehend many CPS attack types better and create countermeasures to lessen their effects.

In a false command injection attack (FCIA), a malicious actor endeavors to maliciously insert an unauthorized command into the targeted network with the intention of inducing a malfunction in the network [15]. In the realm of a smart grid, such adversaries may exploit vulnerabilities at the software, communication channel, or hardware levels to introduce a deceptive command into the system. FCIA incidents can be highly impactful as they specifically target the commands that execute crucial operations. These attacks are not only difficult to detect, but they can cause significant damage before they are detected. This is in contrast to false data injection attacks (FDIAs), which focus on manipulating data from different sensors and measurement nodes within a smart grid [16]. A situation in which a malicious attacker introduces false commands into a power plant's control system to open a relay, disconnect the generator, and cause the plant to shut down is an illustration of an FCIA on a smart grid. FCIAs may result in possible safety risks for plant workers in addition to a power outage and equipment damage. The Stuxnet worm on Iranian nuclear power plants [17], the "Aurora" experiment [18], the attack on the Ukrainian power system in December 2015 [19], and the Maroochy water system attack [20] are examples of major FCIAs on critical infrastructures. Employing the injection and execution of the false command into the crucial application, the attackers were able to seriously harm the targeted system in these attacks. These attacks highlight the vulnerability of critical infrastructure to FCIAs.

A. CPS SECURITY OBJECTIVES

The security of a CPS is ensured by including authenticity in the list of security objectives, in addition to the three fundamental security objectives for information security defined by NIST (confidentiality, integrity, and availability) [21], [22], [23], [24].

1) CONFIDENTIALITY

Confidentiality of a system is defined as its ability to prevent unauthorized individuals or systems from accessing critical information [25]. Confidentiality is crucial for maintaining users' privacy in CPSs, but it is not enough on its own. Data leakage may lead to unauthorized access and misuse of information. Maintaining confidentiality in CPSs requires ensuring that sensitive information, including signals, commands, and configurations, is only accessible to authorized personnel.

TABLE 1. Security Objective Priority Comparison Between Traditional Information Systems and CPS

Priority	Information System	CPS
First	Confidentiality	Availability
Second	Integrity	Integrity
Third	Availability	Confidentiality
Fourth	—	Authenticity

2) INTEGRITY

Integrity refers to the ability to ensure that data or resources cannot be modified without proper authorization [23]. Integrity is compromised when crucial information is maliciously or accidentally altered or deleted, leading to recipients accepting false data as valid. In the context of CPSs, it is necessary to prevent unauthorized modifications to sensitive information shared among various system components.

3) AVAILABILITY

To ensure system effectiveness, it is essential to guarantee accessibility whenever required. This involves ensuring the proper functioning of cyber systems responsible for information storage and processing, physical controls for executing physical processes, and communication channels for accessing these components [26]. In a CPS, high availability guarantees continuous access to essential services by proactively mitigating potential disruptions, such as failures, system upgrades, power outages, and denial-of-service attacks. This involves ensuring the resilience of computing, control, and communication systems to maintain uninterrupted functionality.

4) AUTHENTICITY

The main goal of authenticity in a CPS is to achieve authentication throughout the numerous components as well as the processes of the CPS. Authenticity ensures the legitimacy of the data, communication, and transactions in a CPS. Authenticity aims to validate all the parties involved in a communication [21], [22]. In the context of CPS, achieving authenticity across processes, such as sensing, communications, and actuation, is a primary objective.

The security priorities in CPS are different from those in conventional information systems [27]. In CPSs, availability is critical and has the highest priority, followed by integrity, confidentiality, and finally authenticity, as shown in Table 1.

B. RELATED SURVEYS AND MAIN CONTRIBUTIONS

In the existing literature, several surveys have been carried out to discuss different aspects of cyberattacks on smart grids. The authors in [28] and [29] summarized cyberattacks, detection, and countermeasure techniques in smart grids. A summary of detection techniques for FDIAs using machine learning (ML) is provided in [30]. Similarly, Sahani et al. [31] provided a survey of ML-based intrusion detection systems (IDS) for smart grids. The authors in [16], [32], [33], and [34] focused on summarizing detection techniques specifically for FDIAs in smart grids. The authors in [35] and [36] provided a summary with the futuristic perspective of attacks and countermeasures in smart grids. All these studies either provide a holistic view of cyberattacks and detection mechanisms or focus on a specific category of cyberattacks. To the best of the authors' knowledge, there is no study that provides a review of FCIAs in smart grids. Therefore, this article focuses on providing a comprehensive survey of FCIAs in smart grids. Table 2 draws the comparison among the techniques covered by the existing surveys and the proposed work. It is evident from the table that our work has clearly superior performance compared to all the existing surveys. The main contributions of this article are as follows.

TABLE 2. Comparison Between the Existing Surveys and the Proposed Work

	[28] [32] [36] [37]	[29] [35]	[30] [31]	Proposed Work
AI-based techniques	✓	✗	✓	✓
Model-based techniques	✓	✓	✗	✓
FCIA	✗	✗	✗	✓

1) We provide a classification of FCIAs in smart grids according to the targeted component.
2) We discuss the impacts of FCIAs in smart grids.
3) We provide a summary of existing detection techniques for FCIAs.
4) We identify the strengths and limitations of existing techniques.

C. ARTICLE ORGANIZATION

This article is organized to provide an introduction to CPS attacks with background, objectives, and related work in Section I. Section II provides the literature review methodology adopted for this survey. Section III provides the classification of FCIAs according to the targeted components of a smart grid and elaborates on the impacts of these attacks on smart grids. Detailed classification of detection techniques for FCIAs is provided in Section IV. Comparative analysis of detection techniques with research gaps and future directions is provided in Section V. Finally, Section VI concludes this article.

II. LITERATURE REVIEW METHODOLOGY

This section provides a systematic methodology adapted for conducting the literature review in this survey to comprehensively explore and analyze the existing research on FCIAs in smart grids. This methodology encompasses the articulation of a research objective, formulation of a search strategy, establishment of inclusion criteria, extraction and synthesis of information, and, ultimately, categorization and discussion of the findings. Each of these steps is explicated as follows.

A. RESEARCH OBJECTIVE

The main objective of this survey is to perform a comprehensive review of existing studies on FCIAs in smart grids. The purpose of the survey is to identify major themes, trends, and research gaps in the discipline.

B. SEARCH AND STRATEGY

Various electronic databases, including IEEE Xplore, ScienceDirect, Google Scholar, and the ACM Digital Library, were used to perform a systematic search of relevant literature. The terms "false command injection attacks," "smart grid security," and other combinations of related keywords were used in the search.

C. INCLUSION CRITERIA

Initially, studies were filtered based on titles and abstracts. After that, suitable studies were chosen using the following inclusion criteria:

1) studies targeting FCIAs in smart grids;
2) established journal papers, reputable conference papers, and manuals and reports issued by regulatory bodies.

D. INFORMATION EXTRACTION AND SYNTHESIS

Each chosen study was thoroughly studied to extract relevant information, including types of attacks, their impact, and countermeasures to detect and mitigate these attacks. The proposed technique, experimental design, and relevance to the research problem were used to evaluate the quality of the included studies. The findings from the chosen research were summarized to discover common themes, trends, and gaps in the literature.

E. FINDINGS AND DISCUSSION

The findings of the literature review were organized and presented by categorizing the chosen studies. Attack types, their impact, and detection techniques were used to categorize studies. Discussion on each category highlighting the pros and cons alongside research gaps and future directions were presented.

III. CLASSIFICATION AND IMPACTS OF FCIAS IN SMART GRIDS

The injection of fake commands into the smart grids as a result of FCIA has severe consequences on both the stability and the operation of the smart grids, where an attacker can force the system to pursue wrong decisions. This can lead to power outages, blackouts, hardware failures, synchronization problems, financial loss, and other critical issues in the power grid.

A. CLASSIFICATION OF FCIAS

Cyberattacks against CPSs exploit vulnerabilities in physical systems, cyber systems, and the interfaces between the two. To comprehend and protect against these risks, it is crucial to classify these attacks. This is because it enables researchers and practitioners to distinguish among various attack types and create efficient solutions. Attacks in smart grids have been categorized using a variety of parameters, such as security needs, the design of the grid, the kind of cyberattack, and the target of the attacker. Cyberattacks were categorized by the authors in [37] and [38] using the CIA Triad, which is a set of security requirements based on confidentiality, integrity, and availability. Sakhnini et al. [39] categorized attacks according to three types of attacks: network-based, spoofing, and data injection. The authors in [9] and [35] used the attacking cycle to classify cyberattacks, which includes reconnaissance and scanning. The authors in [40] and [41] classified cyberattacks into topology-, component-, and protocol-based categories. This classification does not include some passive and active attacks, such as eavesdropping and replay attacks. The authors in [38] and [42] also classified cyberattacks based on the type of network, i.e., wide area network, neighborhood area network, personal area network, and field area network. This classification only includes attacks on the network and excludes attacks on other components of the smart grid. Musleh et al. [32] classified cyberattacks based on the delivery method of attacks, including cyber-, network-, communication-, and physical-based attacks. Khoei et al. [28] classified cyberattacks based on the target layer in the open systems interconnection (OSI) model. This classification provides a detailed account of numerous types of cyberattacks on each layer of the OSI model.

While the aforementioned schemes cover a wide range of cyberattacks or concentrate on specific categories, there is currently no specific study dedicated to classifying FCIAs. Thus, it is important to classify FCIAs based on a scheme that helps in analyzing these attacks and their detection schemes. Smart grids, being CPSs, have physical, software, and communication components as their basic ingredients, as shown in Fig. 2. Fig. 3 gives a classification of FCIAs according to these three components. This classification also maps attacks on three components of smart grids to seven layers of the OSI model.

1) HARDWARE-BASED ATTACKS

An attacker may tamper with or damage the physical infrastructure to disrupt or destroy power delivery by injecting false commands into smart grids [43]. For example, an attacker could tamper with an actuator in the control system of a substation to cause a malfunction of the system or disrupt the power supply. An attacker could also physically manipulate the equipment in the power system, such as switchgear, generators, or transformers, potentially causing a widespread power outage. Power generation systems, transmission lines, distribution systems, and energy metering systems are among the potential targets of FCIAs on the physical layer of a smart grid [44], [45].

2) COMMUNICATION-BASED ATTACKS

Smart grids are vulnerable to communication-based FCIAs, which include attacks on the data link, network, and transport

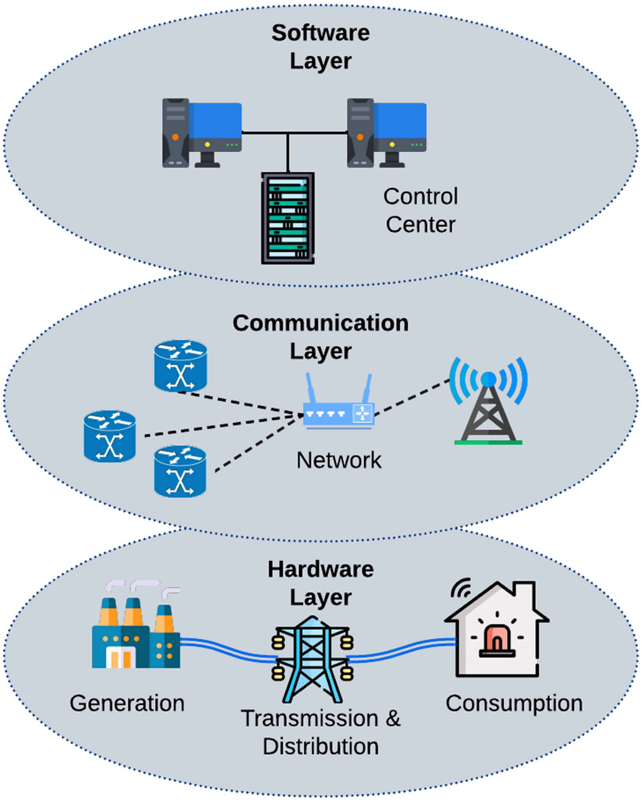

FIGURE 2. FCIAs' target components in the smart grid.

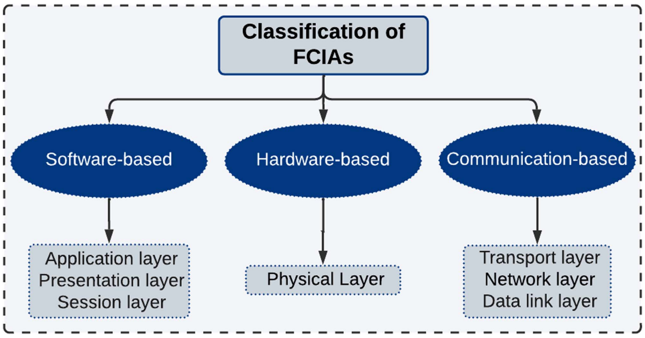

FIGURE 3. Classification of FCIAs.

layers. By sending a false command into the communication system, an attacker could launch an attack on the smart grid. Intercepting communication between devices, such as a substation and a control center, and then inserting malicious commands is an example of this attack [45], [46]. The attacker could combine an FCIA with massive traffic flooding on a network to disrupt legitimate communication [47], [48]. A hacker might also target a transport layer protocol's flaws to sabotage or alter device-level communication. An attacker might, for instance, use a flaw in the transmission control protocol/Internet protocol to introduce false commands into the communication channel, which could lead to a system malfunction [46].

3) SOFTWARE-BASED ATTACKS

These FCIAs in smart grids are mapped onto the OSI model's display, application, and session layers. A smart grid could be manipulated or have its operation disrupted by inserting a false command into the presentation layer by an attacker [49]. Similarly, an attacker may launch a hijacking attack targeting an already-existing session to obtain sensitive data and commands. In the same way, applications and software flaws in the smart grid might also be targeted to obtain unauthorized access and send malicious commands that would interrupt the power supply. For example, control system software could be targeted by the attacker to possibly disrupt and damage the power grid [50].

B. IMPACTS OF FCIAS ON SMART GRIDS

Numerous research works have examined the impacts of FCIAs, which pose significant risks to the smart grid. FCIAs have proven their ability to trigger blackouts, load shedding, and disruptions in the wide area control system in situations similar to those described in [51] and [52]. These events underscore the disruptive impact of FCIAs on the operation of smart grids. Successful FCIAs can cause significant harm to critical infrastructure in addition to operational disruptions; this has been shown in [53], [54], and [55], where attacks on Automated Control for Parallel Generators and cascading FCIAs led to instability and possible grid failures. False demand response commands and designed topology attacks cause increased load, altered pricing, and significant financial losses—up to $100 000 in a single 24-h period—due to increased demand and deliberate topology attacks. These effects have a substantial economic impact, as discussed in [51]. As examined in [56] and [57], the economic effects also affect locational marginal pricing in the energy markets. In smart grids, major impacts of FCIAs include operation disruption, damage to infrastructure, and significant financial losses.

IV. DETECTION TECHNIQUES FOR FCIAS

We propose classifying the FCIA detection methods into two main categories: model- and artificial intelligence (AI)-based methods. To find an FCIA, the AI-based methods employ a variety of data mining, ML, and evolutionary algorithms. In contrast, different mathematical models and estimate techniques are used for detection in model-based approaches. An overview of detection methods for FCIAs is presented in Fig. 4.

A. AI-BASED TECHNIQUES

AI-based FCIA detection methods in smart grids use AI algorithms to find unusual patterns in the command flow that governs the power grid. It is possible to train these detection methods to identify the typical command flow pattern and identify any deviations from it as possibly malicious commands. Furthermore, AI-generated commands are hard to find with conventional detection approaches; these can be found

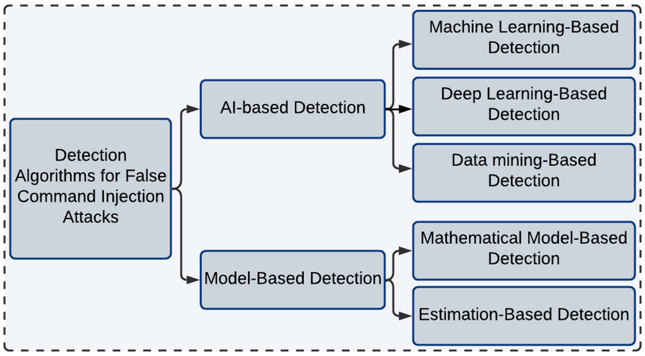
Detection Algorithms for False Command Injection Attacks
AI-based Detection
Model-Based Detection
Machine Learning-Based Detection
Deep Learning-Based Detection
Data mining-Based Detection
Mathematical Model-Based Detection
Estimation-Based Detection

FIGURE 4. Categorization of detection techniques for FCIAs.

with AI-based detection techniques [58].These AI-based detection techniques can also be employed to continuously monitor the operation of a smart grid.

1) ML-BASED TECHNIQUES

ML is one of the most fundamental and important fields in the area of AI. Researchers are increasingly focusing their attention on the utilization of ML-based algorithms for detecting cyberattacks. ML models are trained to learn patterns in past data. Trained models are then used to make a decision based on observed samples without human intervention [59]. A well-trained ML model can perform complex challenging tasks, such as identifying FCIAs in smart grids. ML algorithms can be further categorized into three subcategories: 1) supervised learning; 2) unsupervised learning; and 3) reinforcement learning [60]. In supervised learning, the training data consist of input–output pairs, with the model adjusting parameters to minimize differences between predictions and true values. In unsupervised learning, training lacks output labels, aiming to identify patterns or structures within data for further analysis [61]. Reinforcement learning involves an agent learning decision making through interaction with an environment, utilizing trial and error, feedback in rewards or penalties, and refining its policy to maximize cumulative reward [60]. Various ML algorithms used for FCIA in the literature are discussed in this section [60].

Upadhyay et al. [62] combined the gradient boosting feature selection, a feature selection framework, with the decision tree (DT) algorithm to detect FCIAs on relays in a power system. The proposed prepossessing of data and selection of the most promising features improve the performance of the DT model. Kumar et al. [63] used minority oversampling and feature selection to improve the detection of FCIAs on power systems using ML. Kumar et al. [64] showed that the performance of various ML models to detect FCIAs is dependent on preprocessing and feature selection. Various ML models analyzed include random forest (RF), support vector machine (SVM), Naive Bayes (NB), etc. Sahu et al. [65] demonstrated the application of the data fusion approach on multisource and multidomain data to reduce the false positive rate in intrusion detection. Numerous supervised classification techniques, such as linear regression, NB, RF, and DT, are compared with semisupervised based co-training. They demonstrated the superiority of semisupervised co-training over conventional classification methods.

2) DEEP-LEARNING-BASED TECHNIQUES

Artificial neural networks, the basis for deep learning (DL), are a branch of ML that employs algorithms designed to mimic the structure and operations of the human brain. It is employed in many different applications, including audio and picture identification, natural language processing, and decision making. Convolutional neural networks (CNNs), autoencoders, long short-term memory (LSTM), and deep belief networks (DBNs) are the most widely used DL models. The backpropagation algorithm, a DL approach, was utilized by Gao et al. [66] to identify FCIAs in smart grids. To create an IDS for command and response injection attacks on supervisory control and data acquisition (SCADA) systems, a three-layer neural network is designed. For feature extraction, Potluri and Diedrich [67] employed both the DBN and the stacked autoencoder (SAE). Combining feature extraction from the SAE and the DBN with the SVM and Softmax regression (SMR)-based classification methods is another method. The various assessment metrics for FCIA detection are compared using all four combinations, namely, DBN with SMR, DBN with SVM, SAE with SMR, and SAE with SVM. Qu et al. [68] used CPS attack genes to identify FCIAs in power systems, which is a similar method. Qi et al. [69] suggested combining a number of semisupervised anomaly detection techniques with a deep autoencoder. One kind of neural network that permits the use of prior outputs as inputs for the current task is the recurrent neural network (RNN). This makes it possible for the RNN to process input sequences, such a time series or a text. Natural language processing and speech recognition frequently employ RNNs [70]. Eke et al. [71] used deep ensemble RNNs and CNN to identify response injection and command injection threats in SCADA systems. A DL-based hybrid technique was presented by Bitirgen and Filik [72] to identify command injection attacks that cause remote tripping on relay systems inside a smart grid. Particle swarm optimization is used to optimize CNN–LSTM, a CNN–LSTM combination. The proposed approach has been verified for systems with two, three, and more classes. It makes a clear distinction between cyberattacks and physical disruptions.

3) DATA MINING

Identifying trends and information from vast volumes of data is called data mining. It entails removing meaningless data from raw data by applying statistical models and algorithms to reveal insights. Creating actionable knowledge from data to help with decision making is the aim of data mining. Data exploration, data modeling, data preparation, and result interpretation are some of the processes in the data mining process.

Researchers, scientists, and engineers now use data mining as an essential tool because of the growing availability of vast amounts of data and advancements in processing power. Because it has such a narrow range of applications, data mining for cyberattack detection is regarded as unsophisticated. To identify a remote tripping command injection attack in power systems, Pan et al. [73] employed a data mining approach known as common path mining (CPM). The primary objective of CPM is to identify recurring patterns in the data and comprehend the connections among various data items. After patterns are found, anomaly detection is carried out using the patterns. Intriago and Zhang [74] used a semisupervised learning method and a data mining classifier called the Hoeffding adaptive tree to find the difference between cyberattacks and normal system changes.

B. MODEL-BASED DETECTION

Mathematical models are used in model-based detection of FCIAs in CPSs to find and identify abnormal parameter behavior. This method is predicated on the notion that a system's typical behavior can be described by a collection of mathematical models, and that any departure from the norm can be interpreted as an attack. This method looks for differences in the system's behavior by comparing it with the models while the system is being observed in real time. The system can then issue a warning or take other remedial action to stop the attack from succeeding if a disparity is found. One can obtain the mathematical models required for model-based detection by either simulating the system or by monitoring its typical behavior. The models may be built in control theory, mathematics, or physical laws. A model may recognize various kinds of FCIAs once it is established. One important factor in preventing damage in CPSs is real-time attack detection. This approach could be employed to detect real-time attacks.

A strong tool for simulating and examining distributed and concurrent systems is the Petri net. They have been applied extensively across numerous domains and have shown to be useful instruments for comprehending intricate systems and enhancing their behavior. Mathematically, a bipartite-directed graph with two sets of elements—places and transitions—is referred to as a Petri net model. In a system, the places stand for the buffer storage or resources, and the transitions stand for the actions or occasions that use, create, or consume those resources. To mimic more complicated systems, Petri nets can be modified by adding further components [75]. In [76], one such version known as stochastic Petri net is given to discover the malicious FCIAs on substation automation systems in smart grids. Li et al. [77] proposed a second stochastic Petri-net-based hybrid detection approach for insider command injection risks in smart grids.

Ontology is a method in AI that formally defines concepts and relationships within a specific domain. This technique provides a way to control the level of detail in information and enables the automatic extraction, improvement, and analysis of large amounts of data. Recently, the application of ontology in the electric power sector has become a growing area of research. Numerous ontology-based techniques were seen in various applications of power systems [78], [79], [80]. An ontology-based detection of cyberattacks in SCADA systems is presented in [81]. Albalushi et al. [82] proposed an ontology-based scheme on synchrophasor communication to detect malicious command injection in the smart grid.

Estimation techniques are also used for the detection of cyberattacks in smart grids. In estimation-based techniques, various measurement sets and system parameters are utilized to estimate the required variables. Estimation techniques such as weighted least squares and Kalman filter are used in [83] and [84], respectively. A current-to-voltage ratio index is developed in [15] to detect malicious command injection in the phase-shift control of a transformer. A similar detection scheme is used to detect malicious command injection attacks on the tap of a transformer in transmission lines by Chakrabarty and Sikdar [85]. A detection scheme based on the changes in the covariance matrix of measurement is presented to detect the attack on both phase-shift control and tap change control in [86]. A rule-based scheme is presented in [87] to detect a command injection attack on the SCADA system in a smart grid. The system-model-based rules are designed to detect known as well as unknown attacks.

Synchrophasor technology is playing an important role in advancing monitoring and control systems in smart grids by enabling real-time tracking of system dynamics. Khan et al. [88] proposed the model-based design of synchrophasor specific intrusion detection system (SS-IDS) for command injection attacks. The proposed SS-IDS utilized the model-based rules to detect all the cyberattacks including FCIAs.

V. COMPARATIVE ANALYSIS, RESEARCH GAPS, AND FUTURE DIRECTIONS

It is very important to comparatively analyze the pros and cons of existing detection techniques for FCIAs. This section provides a comparison between the two detection techniques by highlighting the advantages and disadvantages of each of them, as summarized in Table 3. Moreover, based on the limitations of the existing work, future research directions are also provided in this section.

A. COMPARATIVE ANALYSIS

AI-based detection algorithms are quick to detect FCIAs once accurately trained. They also offer a low false alarm rate and high detection rate as they only need real data and do not require highly accurate system parameters to run the detection process. Not requiring the system parameters and the system model is one of the most important advantages of these algorithms as it eliminates the requirement for a complete understanding of the complex physical processes in the system. The scalability of a model refers to its ability to accommodate expansion without compromising performance. AI-based algorithms are highly scalable as they can be easily expanded to process a larger volume of data. On the other hand, AI-based algorithms are merely dependent on historical datasets, as models are trained on these datasets. The availability of

TABLE 3. Advantages and Disadvantages of Different Detection Methods

Detection Technique	Advantages	Disadvantages / Limitations
AI-based detection	• Faster detection times. • Higher detection rate. • Lower false alarm rate. • System parameters not required. • System model not required. • Higher Scalability.	• Higher implementation cost. • Dataset required for training and testing. • Extensive training required. • Advanced hardware required. • Higher computational power required. • Real data may not be available due to privacy concerns. • Performance is dependent on the quality of the dataset.
Model-based detection	• No dataset required. • No training needed. • Higher robustness. • Does not require advanced hardware.	• Complex to design. • Real-time system parameters required. • System model required. • Higher computational power required. • Limited accuracy. • Highly sensitive to system parameters. • Threshold setting is critical. • Limited scalability.

high-quality historical data is one of the major limitations of AI-based detection algorithms. Most of these algorithms are iterative in nature and require advanced hardware to meet the demand for high computational power and large memory space. The privacy of datasets in critical applications is also an important concern.

Model-based detection algorithms, on the other hand, use the system model and parameters to identify FCIAs in the system. Model-based detection algorithms have the significant benefit of being free from dependence on historical data. Thus, these algorithms do not demand additional memory storage for a very large dataset to train the system model. Moreover, because model-based algorithms employ the actual physical processes of the system, these algorithms based on an accurate physical model are more robust as compared with AI-based algorithms. In contrast, the primary disadvantages of model-based algorithms are their reliance on system parameters and the complexity of modeling physical processes. The process of creating accurate models and determining the correct parameters can be time consuming and require specialized knowledge and skills. The system's models or parameters may have mistakes or inaccuracies that lead to inaccurate or untrustworthy results. The accuracy of the underlying mathematical model that is used to represent the system determines the precision of a model-based detection procedure. An overly simplistic model that fails to accurately represent the behavior of the system could cause the algorithm to overlook anomalies or generate false-positive alerts. Furthermore, the model-based detection algorithms may struggle with detecting anomalies that are caused by external factors or events that are not accounted for in the model. Scalability can be limited by the complexity of the model used and the ability to keep it up-to-date with changes in the system. As the system grows in complexity or changes over time, the model may need to be updated or modified, which can be time consuming and require specialized knowledge and skills. Therefore, model-based algorithms are both complex to create and incur higher computational complexity.

B. RESEARCH GAPS AND FUTURE DIRECTIONS

This section discusses the limitations of the existing techniques and research gaps in the area of detecting FCIAs in smart grids and provides future directions to fill these existing gaps.

1) DEVELOPING COMPREHENSIVE FRAMEWORKS FOR MULTIDIMENSIONAL ATTACK DETECTION

Current detection methods primarily concentrate on recognizing isolated attack types like communication-, software-, or hardware-based attacks. However, real-world situations often witness coordinated attacks across various entry points, encompassing various layers and physical devices. Adversaries frequently exploit complex attack vectors, for example, combining a denial-of-service attack with a stealthy command injection later on. Comprehensive detection requires connecting these events in both the cyber and physical realms to uncover larger malicious plans.

Researchers could explore architectural frameworks that integrate domain knowledge with enriched telemetry data using graphs and ontologies. These frameworks can facilitate reasoning across interdependent grid components, enabling the identification of sophisticated distributed attacks. The development of integrated environments tying together various grid data facets remains an ongoing challenge.

2) CREATING AUTHENTIC DATASETS FOR TRAINING AND EVALUATION

The absence of public datasets tailored to FCIAs poses a challenge for standardized benchmarking of emerging techniques. Models are frequently showcased using private utility data or synthetic grids that may not fully capture real-world intricacies.

Constructing open yet realistic datasets could significantly enhance the rigor of evaluations. A coordinated initiative to release anonymized intrusion captures or high-fidelity grid emulations can contribute to reproducibility. Managing privacy and security concerns linked to sharing such data is crucial for progressing research. Moreover, advanced platforms that can combine real-world systems with attack behaviors could help in providing diverse databases.

3) ENHANCING TECHNIQUE RESILIENCE AGAINST ADVERSARIAL ATTACKS

While AI holds promise for FCIA detection, recent studies reveal vulnerabilities in DL systems, making them susceptible to subtly perturbed inputs that can mislead predictions [89], [90]. Future research must focus on fortifying techniques against adversarial false command attacks, which could specifically target and evade learned models.

Two promising directions include adversarial retraining by augmenting normal data with simulated attacks and leveraging model ensembles to mitigate individual manipulation vulnerabilities [91], [92]. Designing systems that offer certifiable robustness guarantees against bounded input perturbations can help ensure worst case detection reliability. Overall, directly incorporating adversarial threat models into FCIA defense strategies is crucial for future advancements.

VI. CONCLUSION

The significance of smart grid network security cannot be overstated, and it is a critical factor in the successful implementation of smart grid systems. The need to create advanced detection algorithms to combat the increasing threat of FCIAs is underscored by an exploration of their history, diversity, and impact. FCIAs can be classified according to the targeted component in the smart grid, i.e., hardware component, software component, and communication component. Various impacts of FCIAs in smart grids include disruption of operation, damage to infrastructure, and financial losses. In the existing literature, detection techniques for FCIAs in smart grids are either based on an AI algorithm or a model-based approach. Each category has its advantages and disadvantages that should be taken into consideration when employing a detection mechanism for FCIAs in smart grids. When developing a detection method for FCIAs in a smart grid, parameters that should be taken into account include detection speed, false alarm rate, computational requirement, hardware requirement, scalability, and dependence on system parameters.

REFERENCES

[1] G. Simard, “IEEE Grid Vision 2050,” *IEEE Grid Vis. 2050*, 2013, pp. 1–93.

[2] R. Ma, H.-H. Chen, Y.-R. Huang, and W. Meng, “Smart grid communication: Its challenges and opportunities,” *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 36–46, Mar. 2013.

[3] J. J. M. Escobar, O. M. Matamoros, R. T. Padilla, I. L. Reyes, and H. Q. Espinosa, “A comprehensive review on smart grids: Challenges and opportunities,” *Sensors*, vol. 21, no. 21, 2021, Art. no. 6978.

[4] M. Faheem et al., “Smart grid communication and information technologies in the perspective of Industry 4.0: Opportunities and challenges,” *Comput. Sci. Rev.*, vol. 30, pp. 1–30, 2018.

[5] R. Borgaonkar, I. A. Tøndel, M. Z. Degefa, and M. G. Jaatun, “Improving smart grid security through 5G enabled IoT and edge computing,” *Concurrency Comput.: Pract. Exp.*, vol. 33, 2021, Art. no. e6466.

[6] M. R. Davoodi, R. Moslemi, W. Song, and J. Mohammadpour, “A fog-based approach to secure smart grids against data integrity attacks,” in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf.*, 2020, pp. 1–5.

[7] J. Ding, A. Qammar, Z. Zhang, A. Karim, and H. Ning, “Cyber threats to smart grids: Review, taxonomy, potential solutions, and future directions,” *Energies*, vol. 15, 2022, Art. no. 6799.

[8] “Presidential Policy Directive—Critical Infrastructure Security and Resilience,” Feb. 2013. [Online]. Available: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[9] Y. Yoldaş, A. önen, S. Muyeen, A. V. Vasilakos, and I. Alan, “Enhancing smart grid with microgrids: Challenges and opportunities,” *Renewable Sustain. Energy Rev.*, vol. 72, pp. 205–214, 2017.

[10] L. James,“Energy sector: More cyber attacks in 2022 than ever before.” 2023. Accessed: Dec. 15, 2023 [Online]. Available: https://www.power-and-beyond.com/energy-sector-more-cyber-attacks-in-2022-than-ever-before-a-a53dfeb9e1a85d8a0710a010c7a7e7d3/

[11] T. Kovanen, V. Nuojua, and M. Lehto, “Cyber threat landscape in energy sector,” in *Proc. 13th Int. Conf. Cyber Warfare Secur.*, 2018, p. 353.

[12] S. Toppa, “U.S. power grid gets attacked almost every four days,” 2015. Accessed: Dec. 20, 2023. https://time.com/3757513/electricity-power-grid-attack-energy-security/

[13] B. Advantage, K. Lab, “The state of industrial cyber security2017,” 2017. https://go.kaspersky.com/rs/802-IJN-240/images/ICSWHITEPAPER.pdf

[14] J. J. Broggi, “Building on executive order 13,636 to encourage information sharing for cybersecurity purposes,” *Harvard J. Law Public Policy*, vol. 37, 2014, Art. no. 653.

[15] S. Chakrabarty and B. Sikdar, “Detection of malicious command injection attacks on phase shifter control in power systems,” *IEEE Trans. Power Syst.*, vol. 36, no. 1, pp. 271–280, Jan. 2021.

[16] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, “A review of false data injection attacks against modern power systems,” *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[17] S. Collins and S. McCombie, “Stuxnet: The emergence of a new cyber weapon and its implications,” *J. Policing, Intell. Counter Terrorism*, vol. 7, no. 1, pp. 80–91, 2012.

[18] POWER, “What you need to know (and don’t) about the AURORA vulnerability,” Sep. 2013. [Online]. Available: https://www.powermag.com/what-you-need-to-know-and-dont-about-the-aurora-vulnerability/

[19] “Cyber-attack against Ukrainian critical infrastructure CISA,” Jul. 2021. [Online]. Available: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

[20] N. Sayfayn and S. Madnick, “Cybersafety analysis of the Maroochy shire sewage spill (preliminary draft),” 2017, pp. 1–29.

[21] Y. Ashibani and Q. H. Mahmoud, “Cyber physical systems security: Analysis, challenges and solutions,” *Comput. Secur.*, vol. 68, pp. 81–97, 2017.

[22] S. Ali, T. Al Balushi, Z. Nadir, and O. K. Hussain, *Cyber-Physical Systems Security*. Cham, Switzerland: Springer, 2018, pp. 1–10.

[23] E. K. Wang, Y. Ye, X. Xu, S. M. Yiu, L. C. K. Hui, and K. P. Chow, “Security issues and challenges for cyber physical system,” in *Proc. IEEE/ACM Int. Conf. Green Comput. Commun./Int. Conf. Cyber Phys. Social Comput.*, 2010, pp. 733–738.

[24] T. Lu, J. Zhao, L. Zhao, Y. Li, and X. Zhang, “Security objectives of cyber physical systems,” in *Proc. 7th Int. Conf. Secur. Technol.*, 2014, pp. 30–33.

[25] S. M. Dibaji, M. Pirani, D. B. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakrabortty, "A systems and control perspective of CPS security," *Annu. Rev. Control*, vol. 47, pp. 394–411, 2019.

[26] S. Parvin, F. K. Hussain, O. K. Hussain, T. Thein, and J. S. Park, "Multi-cyber framework for availability enhancement of cyber physical systems," *Computing*, vol. 95, no. 10, pp. 927–948, Oct. 2013, doi: 10.1007/s00607-012-0227-7.

[27] M. Cheminod, L. Durante, and A. Valenzano, "Review of security issues in industrial networks," *IEEE Trans. Ind. Informat.*, vol. 9, pp. 277–293, 2013. [Online]. Available: https://api.semanticscholar.org/CorpusID:15472749

[28] T. T. Khoei, H. O. Slimane, and N. Kaabouch, "A comprehensive survey on the cyber-security of smart grids: Cyber-attacks, detection, countermeasure techniques, and future directions," 2022. [Online]. Available: https://arxiv.org/abs/2207.07738

[29] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *Int. J. Elect. Power Energy Syst.*, vol. 99, pp. 45–56, 2018.

[30] L. Cui, Y. Qu, L. Gao, G. Xie, and S. Yu, "Detecting false data attacks using machine learning techniques in smart grid: A survey," *J. Netw. Comput. Appl.*, vol. 170, 2020, Art. no. 102808.

[31] N. Sahani, R. Zhu, J.-H. Cho, and C.-C. Liu, "Machine learning-based intrusion detection for smart grid computing: A survey," *ACM Trans. Cyber-Phys. Syst.*, vol. 7, pp. 1–31, 2023.

[32] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2218–2234, May 2020.

[33] H. T. Reda, A. Anwar, and A. Mahmood, "Comprehensive survey and taxonomies of false data injection attacks in smart grids: Attack models, targets, and impacts," *Renewable Sustain. Energy Rev.*, vol. 163, 2022, Art. no. 112423.

[34] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 411–423, Apr. 2017.

[35] Z. E. Mrabet, N. Kaabouch, H. E. Ghazi, and H. E. Ghazi, "Cyber-security in smart grid: Survey and challenges," *Comput. Elect. Eng.*, vol. 67, pp. 469–482, 2018.

[36] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: A survey," *IET Cyber-Phys. Syst.: Theory Appl.*, vol. 1, no. 1, pp. 13–27, 2016.

[37] B. B. Gupta and T. Akhtar, "A survey on smart power grid: Frameworks, tools, security issues, and solutions," *Ann. Telecommun.*, vol. 72, pp. 517–549, 2017.

[38] D. B. Rawat and C. Bajracharya, "Cyber security for smart grid systems: Status, challenges and perspectives," in *Proc. SoutheastCon*, 2015, pp. 1–6.

[39] J. Sakhnini, H. Karimipour, A. Dehghantanha, R. M. Parizi, and G. Srivastava, "Security aspects of Internet of Things aided smart grids: A bibliometric survey," *Internet Things*, vol. 14, 2021, Art. no. 100111.

[40] J. Liu, Y. Xiao, and J. Gao, "Achieving accountability in smart grid," *IEEE Syst. J.*, vol. 8, no. 2, pp. 493–508, Jun. 2014.

[41] F. Aloul, A. Al-Ali, R. Al-Dalky, M. Al-Mardini, and W. El-Hajj, "Smart grid security: Threats, vulnerabilities and solutions," *Int. J. Smart Grid Clean Energy*, vol. 1, no. 1, pp. 1–6, 2012.

[42] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Commun. Surv. Tuts.*, vol. 16, no. 4, pp. 1933–1954, Fourth Quarter 2014.

[43] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan, and U. Adhikari, "Modeling cyber-physical vulnerability of the smart grid with incomplete information," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 235–244, Mar. 2013.

[44] S. N. Islam, Z. Baig, and S. Zeadally, "Physical layer security for the smart grid: Vulnerabilities, threats, and countermeasures," *IEEE Trans. Ind. Informat.*, vol. 15, no. 12, pp. 6522–6530, Dec. 2019.

[45] M. S. Al-kahtani and L. Karim, "A survey on attacks and defense mechanisms in smart grids," *Int. J. Comput. Eng. Inf. Technol.*, vol. 11, no. 5, pp. 94–100, 2019.

[46] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Comput. Netw.*, vol. 169, 2020, Art. no. 107094.

[47] K. Ambili and J. Jose, "Trust based intrusion detection system to detect insider attacks in IoT systems," in *Information Science and Applications*. New York, NY, USA: Springer, 2019, pp. 631–638.

[48] Y. Wang, T. T. Gamage, and C. H. Hauser, "Security implications of transport layer protocols in power grid synchrophasor data communication," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 807–816, Mar. 2016.

[49] W. Yin, P. Hu, J. Wen, and H. Zhou, "ACK spoofing on MAC-layer rate control: Attacks and defenses," *Comput. Netw.*, vol. 171, 2020, Art. no. 107133.

[50] S. Wang, S. Zhu, and Y. Zhang, "Blockchain-based mutual authentication security protocol for distributed RFID systems," in *Proc. IEEE Symp. Comput. Commun.*, 2018, pp. 74–77.

[51] B. Min and V. Varadharajan, "Cascading attacks against smart grid using control command disaggregation and services," in *Proc. 31st Annu. ACM Symp. Appl. Comput.*, 2016, pp. 2142–2147.

[52] J. Chen et al., "Impact analysis of false data injection attacks on power system static security assessment," *J. Modern Power Syst. Clean Energy*, vol. 4, no. 3, pp. 496–505, 2016.

[53] P. Wlazlo et al., "Man-in-the-middle attacks and defense in a power system cyber-physical testbed," *IET Cyber-Phys. Syst.: Theory Appl.*, vol. 6, pp. 164–177, 2021.

[54] M. M. Roomi, S. M. S. Hussain, D. Mashima, E.-C. Chang, and T. S. Ustun, "Analysis of false data injection attacks against automated control for parallel generators in IEC 61850-based smart grid systems," *IEEE Syst. J.*, vol. 17, no. 3, pp. 4603–4614, Sep. 2023.

[55] L. Che, X. Liu, Z. Shuai, Z. Li, and Y. Wen, "Cyber cascades screening considering the impacts of false data injection attacks," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6545–6556, Nov. 2018.

[56] L. Jia, J. Kim, R. J. Thomas, and L. Tong, "Impact of data quality on real-time locational marginal price," *IEEE Trans. Power Syst.*, vol. 29, no. 2, pp. 627–636, Mar. 2014.

[57] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 659–666, Dec. 2011.

[58] K. Hasan, S. S. Shetty, and S. Ullah, "Artificial intelligence empowered cyber threat detection and protection for power utilities," in *Proc. IEEE 5th Int. Conf. Collaboration Internet Comput.*, 2019, pp. 354–359.

[59] P. Kalaharsha and B. M. Mehtre, "Detecting phishing sites—An overview," 2021, *arXiv:2103.12739.*

[60] R. K. Dhanaraj, K. Rajkumar, and H. U., "Enterprise IoT modeling: Supervised, unsupervised, and reinforcement learning," in *Business Intelligence for Enterprise Internet of Things*. Cham, Switzerland: Springer, 2020, pp. 55–79.

[61] J. Qiu, Q. hui Wu, G. Ding, Y. Xu, and S. Feng, "A survey of machine learning for big data processing," *EURASIP J. Adv. Signal Process.*, vol. 2016, pp. 1–16, 2016.

[62] D. Upadhyay, J. Manero, M. Zaman, and S. Sampalli, "Intrusion detection in SCADA based power grids: Recursive feature elimination model with majority vote ensemble algorithm," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 3, pp. 2559–2574, Jul.–Sep. 2021.

[63] A. Kumar, N. Saxena, S. Jung, and B. J. Choi, "Improving detection of false data injection attacks using machine learning with feature selection and oversampling," *Energies*, vol. 15, no. 1, 2021, Art. no. 212.

[64] A. Kumar, N. Saxena, and B. J. Choi, "Machine learning algorithm for detection of false data injection attack in power system," in *Proc. Int. Conf. Inf. Netw.*, 2021, pp. 385–390.

[65] A. Sahu et al., "Multi-source multi-domain data fusion for cyberattack detection in power systems," *IEEE Access*, vol. 9, pp. 119118–119138, 2021.

[66] W. Gao, T. Morris, B. Reaves, and D. Richey, "On SCADA control system command and response injection and intrusion detection," in *Proc. eCrime Res. Summit*, 2010, pp. 1–9.

[67] S. Potluri and C. Diedrich, "Deep learning based efficient anomaly detection for securing process control systems against injection attacks," in *Proc. IEEE 15th Int. Conf. Autom. Sci. Eng.*, 2019, pp. 854–860.

[68] Z. Qu et al., "False data injection attack detection in power systems based on cyber-physical attack genes," *Front. Energy Res.*, vol. 9, 2021, Art. no. 644489.

[69] R. Qi, C. Rasband, J. Zheng, and R. Longoria, "Detecting cyber attacks in smart grids using semi-supervised anomaly detection and deep representation learning," *Information*, vol. 12, no. 8, 2021, Art. no. 328.

[70] S. Kombrink, T. Mikolov, M. Karafiát, and L. Burget, "Recurrent neural network based language modeling in meeting recognition.," in *Proc. Annu. Conf. Int. Speech Commun. Assoc.*, 2011, pp. 2877–2880.

[71] H. Eke, A. Petrovski, and H. Ahriz, “Detection of false command and response injection attacks for cyber physical systems security and resilience,” in *Proc. 13th Int. Conf. Secur. Inf. Netw.*, 2021, pp. 1–8, doi: 10.1145/3433174.3433615.

[72] K. Bitirgen and U. B. Filik, “A hybrid deep learning model for discrimination of physical disturbance and cyber-attack detection in smart grid,” *Int. J. Crit. Infrastruct. Protection*, vol. 40, 2023, Art. no. 100582.

[73] S. Pan, T. Morris, and U. Adhikari, “Developing a hybrid intrusion detection system using data mining for power systems,” *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 3104–3113, Nov. 2015.

[74] G. Intriago and Y. Zhang, “Online dictionary learning based fault and cyber attack detection for power systems,” in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2021, pp. 1–5.

[75] Molloy, “Performance analysis using stochastic Petri nets,” *IEEE Trans. Comput.*, vol. C-31, no. 9, pp. 913–917, Sep. 1982.

[76] A. Hahn and M. Govindarasu, “Model-based intrustion detection for the smart grid (minds),” in *Proc. 8th Annu. Cyber Secur. Inf. Intell. Res. Workshop*, 2013, pp. 1–4, doi: 10.1145/2459976.2460007.

[77] B. Li, R. Lu, G. Xiao, H. Bao, and A. A. Ghorbani, “Towards insider threats detection in smart grid communication systems,” *IET Commun.*, vol. 13, no. 12, pp. 1728–1736, 2019.

[78] D. Schachinger, W. Kastner, and S. Gaida, “Ontology-based abstraction layer for smart grid interaction in building energy management systems,” in *Proc. IEEE Int. Energy Conf.*, 2016, pp. 1–6.

[79] Y. Huang and X. Zhou, “Knowledge model for electric power big data based on ontology and semantic web,” *CSEE J. Power Energy Syst.*, vol. 1, no. 1, pp. 19–27, 2015.

[80] D. Wang, W. H. Tang, and Q. H. Wu, “Ontology-based fault diagnosis for power transformers,” in *Proc. IEEE PES Gen. Meeting*, 2010, pp. 1–8.

[81] D. Krauß and C. Thomalla, “Ontology-based detection of cyber-attacks to SCADA-systems in critical infrastructures,” in *Proc. 6th Int. Conf. Digit. Inf. Commun. Technol. Appl.*, 2016, pp. 70–73.

[82] A. Albalushi, R. Khan, K. McLaughlin, and S. Sezer, “Ontology-based approach for malicious behaviour detection in synchrophasor networks,” in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2017, pp. 1–5.

[83] J. Zhao et al., “Power system dynamic state estimation: Motivations, definitions, methodologies, and future work,” *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 3188–3198, Jul. 2019.

[84] A. Monticelli, “Electric power system state estimation,” *Proc. IEEE*, vol. 88, no. 2, pp. 262–282, Feb. 2000.

[85] S. Chakrabarty and B. K. Sikdar, “Detection of hidden transformer tap change command attacks in transmission networks,” *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5161–5173, Nov. 2020.

[86] S. Chakrabarty and B. Sikdar, “Unified detection of attacks involving injection of false control commands and measurements in transmission systems of smart grids,” *IEEE Trans. Smart Grid*, vol. 13, no. 2, pp. 1598–1610, Mar. 2022.

[87] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, B. Pranggono, and H. F. Wang, “Intrusion detection system for IEC 60870-5-104 based scada networks,” in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2013, pp. 1–5.

[88] R. Khan, A. Albalushi, K. McLaughlin, D. Laverty, and S. Sezer, “Model based intrusion detection system for synchrophasor applications in smart grid,” in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2017, pp. 1–5.

[89] D. Gopinath, G. Katz, C. S. Pasareanu, and C. Barrett, “DeepSafe: A data-driven approach for checking adversarial robustness in neural networks,” 2020, *ArXiv:vol. abs/1710.00486, 2017*.

[90] Y.-L. Tsai, C.-Y. Hsu, C.-M. Yu, and P.-Y. Chen, “Formalizing generalization and adversarial robustness of neural networks to weight perturbations,” *in Proc. Int. Conf. Neural Inf. Process. Syst.*, 2021, vol. 34, pp. 19692–19704.

[91] C. Si et al., “Better robustness by more coverage: Adversarial training with mixup augmentation for robust fine-tuning,” Findings Assoc. Computational Linguistics: ACL-IJCNLP 2021, 2021, pp. 1569–1576.

[92] D. Li and Q. Li, “Adversarial deep ensemble: Evasion attacks and defenses for malware detection,” *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 3886–3900, 2020.

MUHAMMAD USAMA received the bachelor’s degree from the National University of Computer and Emerging Sciences, Islamabad, Pakistan, in 2015, and the master’s degree from the Lahore University of Management Sciences, Lahore, Pakistan, in 2018, both in electrical engineering. He is currently working toward the Ph.D. degree in computer engineering at the department of computer science and engineering, University of Nebraska–Lincoln, Lincoln, NE, USA.

His research interests include the security of critical infrastructures, hardware security for reconfigurable devices, and machine learning applications for improving cyber-physical security.

MUHAMMAD NAVEED AMAN (Senior Member, IEEE) received the B.Sc. degree in computer systems engineering from the University of Engineering and Technology, Peshawar, Pakistan, in 2006, the M.Sc. degree in computer engineering from the Center for Advanced Studies in Engineering, Islamabad, Pakistan, in 2008, and the M.Eng. degree in industrial and management engineering and the Ph.D. degree in electrical engineering from the Rensselaer Polytechnic Institute, Troy, NY, USA, in 2012.

He is currently an Assistant Professor with the University of Nebraska–Lincoln, Lincoln, NE, USA, where he also heads the Goof-Proof Hardware-Oriented Security and Trust Lab. Previously, he was an Assistant Professor with the National University of Computer and Emerging Sciences, Islamabad, Pakistan. He was also a Senior Research Fellow with the School of Computing, National University of Singapore, Singapore. His noteworthy research achievements include pioneering device attestation algorithms, innovative approaches to physical layer security leveraging transceiver and wireless channel characteristics, and contributions to understanding privacy attacks on machine learning models. His interdisciplinary expertise extends to blockchains, power systems, optimization, and control systems. His research interests include hardware systems security in embedded devices, physical layer security for Internet of Things devices, and trustworthy machine learning.