IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 10 February 2024, accepted 20 February 2024, date of publication 27 February 2024, date of current version 28 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3370911

TOPICAL REVIEW

A Review on the Evaluation of Feature Selection Using Machine Learning for Cyber-Attack Detection in Smart Grid

SAAD HAMMOOD MOHAMMED[1], ABDULMAJEED AL-JUMAILY[2], (Senior Member, IEEE), MANDEEP S. JIT SINGH[1], VÍCTOR P. GIL JIMÉNEZ[2], (Senior Member, IEEE), AQEEL S. JABER[3], YASEEIN SOUBHI HUSSEIN[4], MUDHAR MUSTAFA ABDUL KADER AL-NAJJAR[5], AND DHIYA AL-JUMEILY[6], (Senior Member, IEEE)

[1]Department of Electrical, Electronic and Systems Engineering, Faculty of Engineering and Built Environment, Universiti Kebangsaan Malaysia, Bangi, Selangor 43600, Malaysia
[2]Department of Signal Theory and Communications, Universidad Carlos III de Madrid, 28911 Leganés, Spain
[3]Independent Researcher, Helsinki, Finland
[4]Department of Information Systems and Computer Science, Ahmed bin Mohammed Military College (ABMMC), Doha, Qatar
[5]Department of Management and Tourism Studies, Oman Tourism College, Muscat 111, Oman
[6]School of Computer Science & Mathematics, Liverpool John Moores University, L3 5AH Liverpool, U.K.

Corresponding authors: Dhiya Al-Jumeily (d.aljumeily@ljmu.ac.uk) and Abdulmajeed Al-Jumaily (abdulmajeed@tsc.uc3.es)

ABSTRACT The Smart Grid is a modern power grid that relies on advanced technologies to provide reliable and sustainable electricity. However, its integration with various communication technologies and IoT devices makes it vulnerable to cyber-attacks. Such attacks can lead to significant damage, economic losses, and public safety hazards. To ensure the security of the smart grid, increasingly strong security solutions are needed. This paper provides a comprehensive analysis of the vulnerabilities of the smart grid and the different approaches for detecting cyber-attacks. It examines the different vulnerabilities of the smart grid, including system vulnerabilities and cyber-attacks, and discusses the vulnerabilities of all its elements. The paper also investigates various approaches for detecting cyber-attacks, including rule-based, signature-based, anomaly detection, and ma-chine learning-based methods, with a focus on their effectiveness and related research. Finally, prospective cybersecurity approaches for the smart grid, such as AI approaches and blockchain, are discussed along with the challenges and future prospects of cyberattacks on the smart grid. The paper's findings can help policymakers and stakeholders make informed decisions about the security of the smart grid and develop effective strategies to protect it from cyber-attacks.

INDEX TERMS Smart grid, cyber-attacks, detection methodologies, anomaly detection, machine learning, future prospects.

I. INTRODUCTION

The Smart Grid is an advanced and integrated power system that relies on sophisticated computer and communication technologies to ensure efficient, reliable, and sustainable electricity supply. However, the integration of these technologies makes the Smart Grid vulnerable to cyber-attacks, which can have serious implications for national security, economic stability, and public safety [1]. These attacks can disrupt the entire grid system, damage physical infrastructure, and compromise confidential information. As a result, ensuring the security of the Smart Grid is crucial for its successful implementation and operation. In recent years, the frequency and sophistication of cyber-attacks on the Smart Grid have increased significantly [2]. These attacks can target various components of the Smart Grid, such as software, hardware, data transfer systems, and operational procedures. Moreover, the introduction of new technologies and the increasing use

The associate editor coordinating the review of this manuscript and approving it for publication was Ahmed F. Zobaa.

of IoT devices have expanded the attack surface of the Smart Grid, making it even more vulnerable to cyber-attacks [3]. To address these challenges, various detection methodologies have been proposed to detect and prevent cyber-attacks on the Smart Grid [4]. These methodologies range from rule-based and signature-based approaches to more advanced anomaly detection and machine learning-based methods [5]. However, the effectiveness of these approaches varies, and new and more sophisticated attacks require more advanced and reliable detection methodologies [6]. In this paper, we provide a comprehensive review of the vulnerabilities of the Smart Grid, including system vulnerabilities and cyber-attacks. We also review the different detection methodologies introduced in previous studies, with a focus on their effectiveness and limitations. Furthermore, we discuss the prospective cybersecurity approaches for the Smart Grid, such as AI and blockchain, and their potential benefits and challenges. Finally, we present the future prospects of cyber-attacks on the Smart Grid, based on recent research and technological advancements as show in Figure 1.

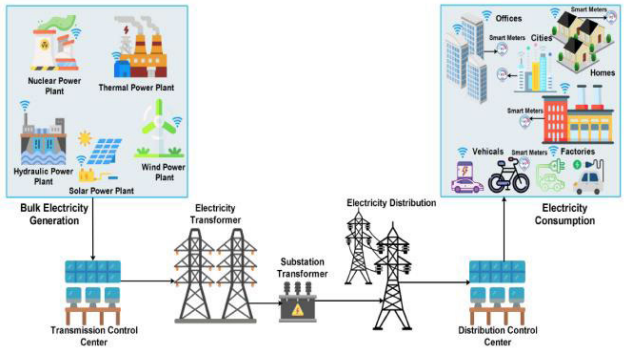

FIGURE 1. Smart grid features [7].

II. RESEARCH BACKGROUND

A smart grid is a vital national infrastructure that employs information and communication technologies to deliver reliable and efficient power transmission and distribution. However, smart grids are vulnerable to cyber-attacks due to their integration of physical and cyber space [8]. For instance, the 2015 Black Energy attack on Ukraine's electricity infrastructure left around 700,000 users without power, highlighting the need for fast response to cyber-attacks [9]. Given the wide variety of attacks, it is essential to classify them to enable appropriate responses. Two primary approaches for detecting attacks are using an attack sample library to match and typical machine learning methods [10]. While the attack sample library can effectively recognize known attacks, it is limited in identifying new attacks not previously recorded in the library [11]. On the other hand, traditional machine learning can recognize and classify new types of attacks by learning from attack samples [12]. However, the success of traditional machine learning algorithms heavily relies on feature engineering, which may be problematic if the attacker conceals these attributes, reducing the effectiveness of the machine learning model [13].

Cyberattacks against smart grid CPSs, an essential infrastructure of all countries, have recently become more prevalent [14]. These attacks pose security challenges such as theft of sensitive data, insertion of fraudulent data, and loss of assets and information through compromised physical devices controlled by supervisory control and data acquisition (SCADA) systems [15]. Detecting these intrusions early is crucial to safeguard smart grid equipment and data, but existing research on intrusion detection systems in smart grids is inadequate [16]. Various machine learning (ML) algorithms that use supervised or unsupervised methods have been proposed in recent years to maintain the cybersecurity of smart grids by categorizing cyberattacks based on different network properties [17]. ML techniques are popular because they can scale to larger systems at a low computational cost. However, selecting the right features and parameters can significantly improve the computing efficiency of any ML method [18]. Many studies have presented ML-based techniques for identifying false data injection (FDI) assaults, such as anomaly detection techniques and support vector machines, which were effective in detecting FDI assaults based on statistical discrepancies in data [19]. Additionally, other methods such as k-nearest neighbors (KNN), single-layer perceptron, and linear and Gaussian support vector machine (SVM) were used as supervised learning techniques to compare and evaluate their performance in detecting FDI assaults [20]. Although these techniques have shown promise in identifying FDI assaults, there is a need for extensive cross-validation among algorithms with varied parameters, and testing should be conducted on power systems of varying sizes to assess the adaptability of the categorization algorithms [21].

One potential solution to the complex problem of identifying and categorizing cyberattacks is the use of neural networks. By employing deep network design, neural networks can extract high-dimensional characteristics, resulting in improved robustness and generalization performance [22], [23], [24], [25], [26], [27], [28]. Additionally, the smart grid's unique ability to communicate with itself provides advantages in terms of effective energy utilization and distribution for a variety of smart devices and machines [29], [30], [31], [32]. However, because the smart grid may store sensitive information, cybersecurity is crucial, and a variety of security solutions must be evaluated and analyzed [33], [34], [35]. Although the smart grid uses communication and information technology to generate, distribute, and consume electricity, there are potential disadvantages such as compromised reliability during power outages and potential privacy concerns if critical data is lost or stolen [36], [37]. One growing method of cyberattack against smart grids is FDI, which can be difficult to detect using current methods [38], [39]. As an alternative to FDI detection, machine learning has been proposed. Injection attacks can also lead to the security breach of an entire web server, resulting in a denial-of-service attack [39], [40].

Hybrid systems are widely applied in industries such as aerospace, energy systems, and industrial control to achieve various objectives by using feedback functions from a specific family [41]. A methodology for developing and accessing a supervisory hybrid control scheme for a microgrid system is presented in [41], using a specialized configuration that includes wind power conversion technology [42], [43]. The microgrid system is represented as a probabilistic hybrid system with many functions for energy management, as depicted in [44]. A formal link between microgrids and stochastic hybrid systems has been established [45], while a state variable modeling technique is used to develop a hybrid large-scale system model of a microgrid system [46]. An intrusion detection system based on network measurements for detecting WBAN jamming attempts was introduced in [47], which employed deep neural networks (DNN) to reduce feature dimensionality [48].

TABLE 1. Existing methods performance.

Ref.	Method	Dataset	Performance
[49]	Correlation-based feature selection and SVM	Smart Grid Dataset	Outperformed other feature selection methods in terms of classification accuracy.
[50]	LASSO and SVM	Smart Grid Dataset	Achieved high classification accuracy and reduced feature dimensionality.
[51]	PCA and SVM	Smart Grid Dataset	Improved classification accuracy and reduced feature dimensionality.
[52]	PCA and SVM	Smart Grid Dataset	Achieved high classification accuracy and reduced feature dimensionality.
[53]	MRMR and SVM	Smart Grid Dataset	Outperformed other feature selection methods in terms of classification accuracy.
[54]	Relief and SVM	Smart Grid Dataset	Improved classification accuracy and reduced feature dimensionality.
[55]	Correlation-based feature selection and SVM	Smart Grid Dataset	Outperformed other feature selection methods in terms of classification accuracy.
[56]	PCA and SVM	Smart Grid Dataset	Achieved high classification accuracy and reduced feature dimensionality.
[15]	CFS and SVM	Smart Grid Dataset	Improved classification accuracy and reduced feature dimensionality.
[57]	Mutual information and SVM	Smart Grid Dataset	Achieved high classification accuracy and reduced feature dimensionality.
[55]	PSO and SVM	Smart Grid Dataset	Improved classification accuracy compared to other feature selection methods.
[58]	Genetic algorithm and SVM	Smart Grid Dataset	Achieved high classification accuracy and reduced feature dimensionality.

The authors of [59] proposed a methodology called deep adversary learning (DAL) to detect network penetration by employing statistical learning and signals. The classifier's objective is to decline intrusion improved data, whereas the producer generates intrusion enhanced datasets. SVM are used to differentiate between the dataset of the attack and normal incursion. The performance of the intrusion detection rate may be improved further by using a deep migrating training model with four steps: ideal feature, variables, knowledge, and feature sampling [60]. The researchers of [61] proposed a five-level restricted Boltzmann machine (RBM) model for identifying Distributed Denial of Service (DDoS) attacks in datasets from applications for smart cities, while [62] integrated the geometric differential module (GDM) and GDM/AG with a deep learning neural network structure to enhance the accuracy and detection of automobile security breaches. Table 1 provides a summary of various existing approaches.

Intrusion detection system (IDS)-based interruption recognition systems have exhibited great promise in certain scenarios [63]. However, to obtain critical information, IDS must be complemented with dynamic system monitoring tools along with traditional security components such as firewalls and antivirus software. To detect FDI attacks, many proposed detection systems employ spatial-transient links, continuous connections, and factual connections of meter estimates [64], [65]. The authors of [66] provide multiple strategies for FDI attack detection using state estimation. The connection between FDI and tiny signal/transient stability requires further investigation for future research. The broad area measuring system is widely used in the current power grid to detect power system irregularities.

The phasor measuring Units (PMUs) are transmitted to the control center for monitoring and damping [67]. FDI attacks can compromise communication between the PMU and the control center, reducing inter-area oscillation dampening and causing small-signal instability. Hence, sophisticated AI systems are needed. Several ML approaches have been recently implemented to detect cyberattacks on a smart grid [68]. For identifying cyberattacks in a CPS, the authors of [69] utilized KNN, decision trees, bootstrap aggregation, and random forest. An auto-associative kernel regression model was utilized to enhance detection performance. Wang et al. [70] advocated using recurrent neural networks with long short-term memory to anticipate the types of cyberattacks.

According to [71] and [72], random forest outperforms SVM and KNN for detecting anomalies in clean water supply systems. In [73], He et al. utilized various ML techniques to evaluate traffic data to identify assaults on thermal power production plants. Numerous studies have employed ML for anomaly/attack detection in SCADA systems, with varying degrees of effectiveness. Comprehensive reviews of these investigations are provided in [74] and [75]. However, previous research did not consider cross-validation of algorithms with variable parameters for detecting cyberattacks in smart-grid settings.

Additionally, ML algorithms are generally assessed on a single smart-grid scenario and may not be applicable to smart grids of various sizes. Secondary systems in smart grids are vulnerable, making security crucial. Previously, machine learning-based approaches have been presented for detecting smart grid assaults. For example, the authors of [76]

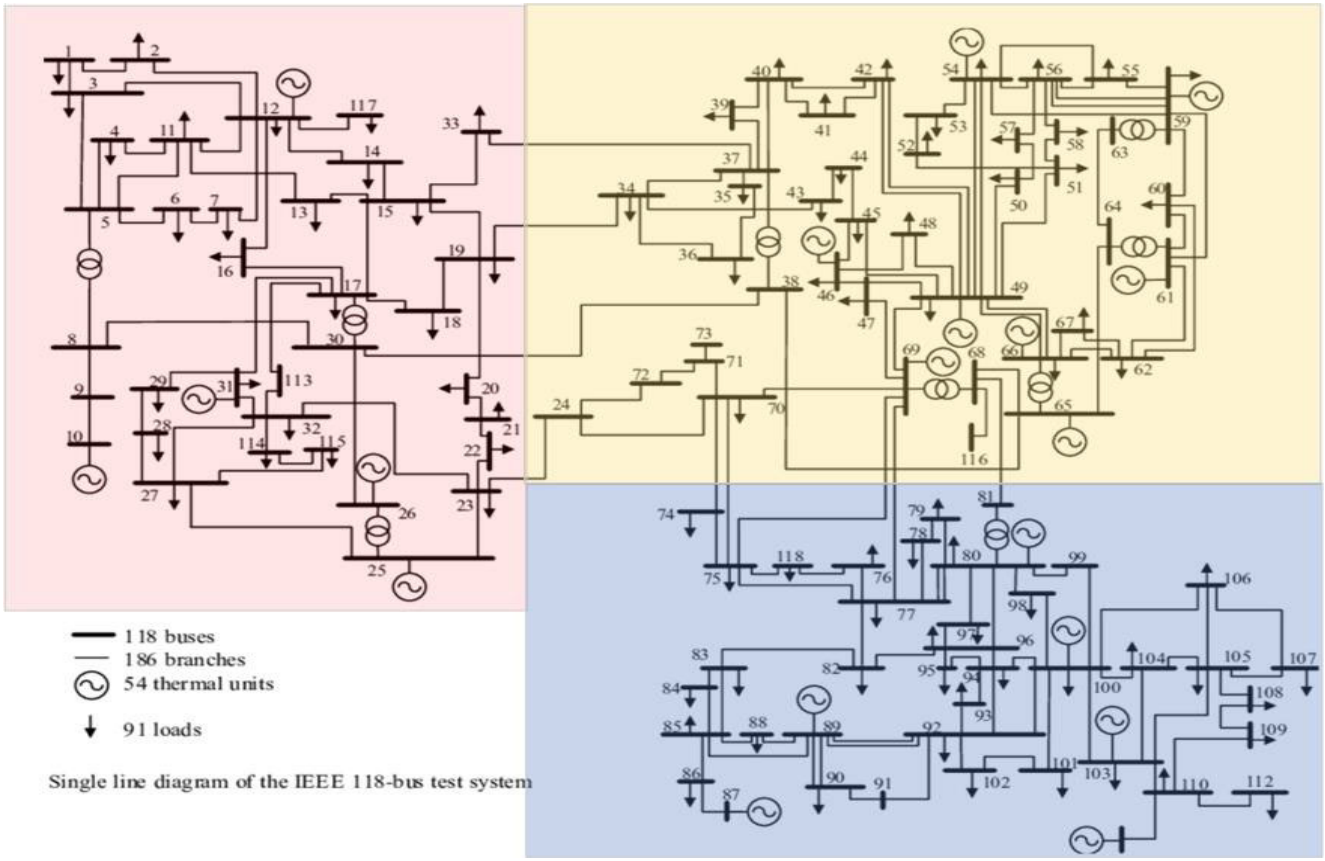

FIGURE 2. IEEE 118 bus test system [77].

developed a method based on classical machine learning methods that used KNN and SVM algorithms to classify assaults and explored online learning techniques for various attack situations.

In [78], the authors suggested a supervised learning-based approach that trains a distributed SVM to detect smart grid threats. The authors of [79] developed a deep learning-based cyberphysical technique using a DBN to prevent data corruption in WAMSs and evaluated performance through simulation. The authors of [80] proposed deep learning algorithms that utilize Conditional DBN to identify aspects of FDI attack behavior using historical measurement data. They also introduced a Long Short-Term Memory neural network in [81] to identify fraudulent input in smart terminals. FDI attacks are a prevalent type of smart grid cyber-attack [82]. Currently, it is challenging to identify FDI attacks that use subpar data detection technology. Machine learning has been suggested in the past to detect FDI attacks. A study [26], [104] investigates three distinct feature selection (FS) procedures and focuses on three varied supervised learning strategies. To test these approaches, IEEE 14-, 57-, and 118-bus systems are utilized as shown in Figure 2.

The accuracy of detection methods for identifying specific threats is often compared. The integration of supervised learning and heuristic feature selection approaches in simulations has led to improved functionality of FDI attack detection systems [83]. Through simulations on a high-fidelity smart grid test bed, it has been demonstrated that machine-learned features can identify SCADA breaches in power transmission systems. Figure 3 illustrates a sample study on the defense system against FDI attacks, based on a conceptual and functional analysis of SCADA [84].

With the incorporation of Information and communication technologies (ICT), the traditional electrical grid is evolving into a smarter grid. However, the smart grid is vulnerable to cyber-attacks, with FDI attacks being among the most severe [85]. To detect such attacks, various ML techniques are under investigation [86]. Nevertheless, the skewed class distribution of the dataset presents a challenge, and prompt response is essential in a smart grid. Fake data injection attacks aim to disrupt microgrid power transmission by providing false information [87]. To combat state estimate attacks, data-driven machine learning is utilized, and ensemble classifiers are employed for classification [88].

Both supervised and unsupervised classifiers are utilized in this approach [89]. The evaluation of this technique is performed through simulation using IEEE 14-bus data [90]. The performance of specific and ensemble models is compared, with the latter outperforming individual classifiers in unsupervised models. Additionally, supervised learning may be used to detect malicious communications and assess their security risks. The Internet of Things (IoT) is a concept

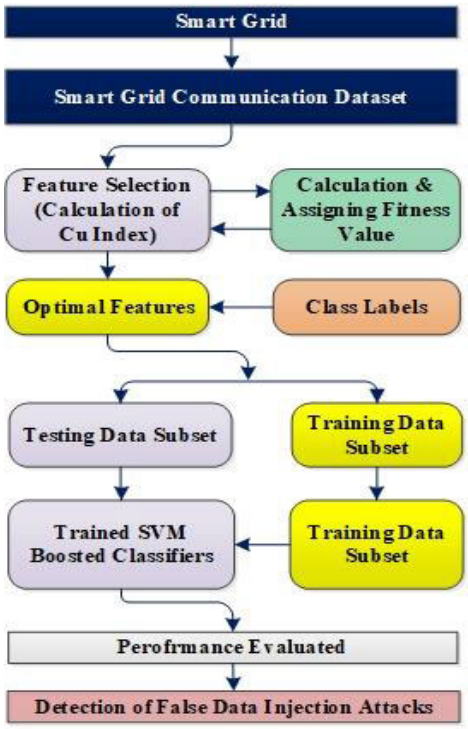

FIGURE 3. Smart grid protection through cyber-malware detection employing efficient and new machine learning techniques.

that seeks to connect people and things with any network and level of support, anytime and anywhere, through various means [91], [92]. IoT has numerous applications and is characterized by a four-layer architecture, as shown in Figure 4. It aims to seamlessly integrate the physical and digital worlds through a networking system of real-world objects equipped with sensors [45], [93].

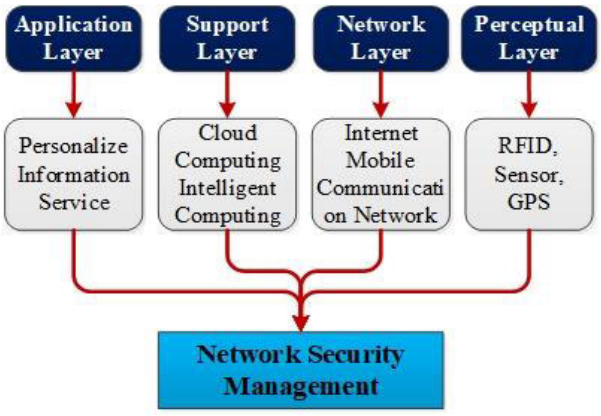

FIGURE 4. Frameworks of IoT [5].

The Internet of Things (IoT) refers to the connection of physical and technological objects over the internet. However, as IoT devices become more common, so do Denial of Service (DoS) and spoofing attacks. Reference [94] have examined IoT network data using classification methods and supervised feature selection approaches. The smart grid security technologies, which were initially thought to be secure, have failed to meet modern cybersecurity requirements. Various tools and methods are required to tackle cyber threats. AI and data modeling may transform the security industry, as they can detect unknown threats using ML algorithms that adjust to a subject's baseline attitude. Reference [35] discuss how technical improvements have shaped the contemporary electrical grid, with debates over its reliability, safety, and efficacy. The smart grid has the potential to increase dependability, visibility, efficiency, and control, but communication within it is critical, and hackers are becoming more interested in smart grid fraud. Cybersecurity and vulnerability risks associated with the smart grid are discussed in a report [95], which addresses attacks and provides responses. The security issues associated with smart grid communications networks, systems, and gadgets are becoming more common, and this research helps readers understand how to detect illegal sensor information tampering. ML algorithms have replaced residual based Bad Data Detection (BDD) in the detection of illegal sensor information tampering.

Semi-supervised anomaly detection methods using PMU data have been employed to identify cyber risks in smart grids. Cyberattacks on SCADA systems are particularly destructive and must be handled with utmost care. DML has been used to overcome intrusion prevention challenges, and the intrusion detection approach based on Deep Machine Learning (DML) has an accuracy rate of roughly 90.0 percent. The authors of [96] have enhanced the detection process by shifting the defensive aim from rejecting assaults to preventing outages, and the authors of [97] have evaluated the impact of a cyberattack on the PMU state estimation procedure.

The authors of [98] presented a defect detection, classification, and placement strategy in radial distribution systems based on sophisticated machine learning techniques. A lightweight technique was proposed in [99], [100], and [101] to detect aberrant state assessments in smart grids produced by FDI assaults in real-time by investigating the spatial-temporal connections between grid state estimations and using trust-voting. Chi-square sensor and cosine resemblance matching techniques were studied in [102] for detecting cyber assaults in smart grids. An adaptable cumulative sum technique for detecting FDI assaults in real-time was devised by the authors of [103].

Recently, machine learning (ML) has been popular for identifying cyber assaults in smart grids, with most suggested systems relying on supervised learning algorithms. [76] used ensemble learning and feature-level fusion with common supervised algorithms like KNN, SVMs, and SLR to anticipate FDI assaults. The authors of [101] examined SVM, KNN, and expanded nearest neighbor (ENN) for clarifying the FDI attacks in smart grids.

In [104], an abnormality detection system was suggested that used a decision tree-based approach based on PMU data to differentiate between normal tripping and power line failures and malicious assaults physically tripping connections. An Adaboost-based classification method was created

in [105] using the random forest as the basic classifier for identifying power system problems and cyber threats utilizing individual PMU data.

Feature engineering procedures, such as feature selection, have been studied in previous research to increase detection performance and minimize computing complexity [78], [106], [107]. In [108] created an intrusion detection module for detecting malicious assaults in the SCADA system using network traces. They used One-Class support vector machine (OCSVM) with K-means recursive clustering to identify intrusions in SCADA systems in real-time [109]. Reference [26] investigated three distinct supervised learning strategies to be employed in conjunction with three distinct Feature Selection (FS) techniques. These approaches are evaluated for adaptability on 118-bus systems, 57-bus, and IEEE 14-bus. The simulation study shows that supervised learning mixed with heuristic FS approaches results in enhanced classification algorithm performance for FDI attack detection. SVM, KNN, and Artificial Neural Network (ANN) are the three ML methods employed. Heuristic FS approaches can pick a subset of features to achieve improved classification accuracy with a much smaller number of features.

The classification of feature selection techniques includes three main categories: filter, wrapper, and embedding approaches. Filter approaches evaluate characteristics individually, utilizing statistical metrics such as correlation, information gain, or chi-square. Wrapper approaches assess feature subsets by integrating the performance of the learning process, often by training and testing the model with various subsets. Embedded approaches incorporate feature selection inside the model training process, optimizing features as an integral component of the overall learning procedure. Genetic Algorithms (GA) are significant in the field of evolutionary computation for their ability to optimize feature subsets through the simulation of natural selection. Within the framework of a smart grid, GA has been utilized for the function of feature selection. This application was examined in research that aimed to discover pertinent attributes for machine learning models by utilizing smart grid data [110]. Genetic programming (GP) utilizes tree topologies to describe alternative solutions and employs evolutionary operations such as crossover and mutation. GP has been implemented in smart grids to optimize demand response, as demonstrated in research [111]. Ant Colony Optimization (ACO) is a prominent evolutionary computation approach that draws inspiration from the foraging behavior of ants, employing swarm intelligence. ACO has been utilized in machine learning to efficiently find subsets of features, hence improving the interpretability of models [112]. Evolutionary computing techniques are crucial in optimizing feature subsets, leading to improved model performance and interpretability in diverse applications such as smart grids and machine learning [113]. Their use demonstrates their efficacy in addressing feature selection issues in intricate datasets [114].

Furthermore, Feature extraction is an essential first step in machine learning [115], with the aim of converting raw data into a more manageable and useful format. This procedure entails the careful selection and modification of pertinent data with the aim of lowering complexity, improving computing effectiveness, and minimizing the likelihood of overfitting [116]. These include linear methods like principal component analysis (PCA) and non-linear methods like t-distributed stochastic neighbor embedding (t-SNE), which is an unsupervised non-linear dimensionality reduction technique for exploring and visualizing high-dimensional data, and autoencoders [117]. These are all types of artificial neural networks (ANNs) that are used to learn how to code unlabeled data efficiently through unsupervised learning. An autoencoder learns two functions: an encoding function that transforms the input data, and a decoding function that recreates the input data from the encoded representation. Feature extraction is utilized in several fields, including computer vision, natural language processing, and signal processing, to enhance model performance and interpretability. Nevertheless, there are obstacles to overcome, such as the risk of information loss during the extraction process and the requirement for meticulous algorithm selection. The PCA can be used to slice data into smaller linear pieces [56], t-SNE can be used to see relationships that don't follow a straight line [118], and autoencoders can be used to get features [119].

Several research possibilities exist to develop antennas with better radiation qualities and innovative ways for producing circular polarization radiation with a broad ARBW that is small in size and covers all necessary bands, as covered in [120]. In [41], the author highlighted a significant advancement approaching the potential implementation of smart grids., operating as a composite system based on cyber-physical concepts. The suggested modeling technique proposes an active paradigm for the management construction of complicated energy systems, aiming to help the environment, technical performance, and economic value. The model was validated by running it through a virtual test bench and studying its reaction throughout an operational range, providing a thorough demonstration of the suggested technique.

The system may run and switch between modes to provide maximum dependability in the face of variable dynamics and load demand. The model uses historical and log data to identify attacks, and the unsupervised machine learning technique is advantageous for identifying zero-day attacks. However, it is prone to false positives, and supervised learning can significantly improve detection confidence. To enhance the feature construction process, the authors analyzed the raw data in the electrical network and generated 16 new features by combining attributes. The authors of [12] proposed a unique strategy for developing a deep neural network that can categorize cyberattacks in smart grids by generating attack behaviors and anticipating the type of assault based on the received message.

In [84], an unsupervised feature learning approach was developed to detect threats in transmission SCADA systems, which improves the accuracy of detection while relying less on system modeling and human knowledge. The approach proposed in [121] identifies new data characteristics that were previously unavailable for 1D power system measurements, leading to further performance improvements. Unlike previous works, which focused primarily on binary classification solutions, the system in [121] addresses the issue of detecting FDI attacks as a problem of multi-class classification, with Convolutional Neural Network (CCN) serving as a multi-label predictor. In [122], a machine learning strategy was presented to detect and protect smart grids against False Data Injection Attacks (FDIA),, which merged feature selection and machine learning. The authors used supervised machine learning models to implement hybrid approaches and compared the suggested model in terms of accuracy, precision, recall, and F1 score.

A. SMART GRID VULNERABILITIES

The Smart Grid is vulnerable to various types of attacks, including cyber-attacks, physical attacks, and human errors. These vulnerabilities can be classified into two categories: system vulnerabilities and cyber-attacks. System vulnerabilities refer to weaknesses in the Smart Grid's physical infrastructure and operational procedures. These vulnerabilities can be caused by outdated or poorly maintained hardware, inadequate security measures, or inadequate training of personnel. For example, outdated software or hardware components may contain security vulnerabilities that can be exploited by attackers to gain unauthorized access to the Smart Grid. Similarly, inadequate security measures, such as weak passwords or lack of encryption, can make the Smart Grid vulnerable to attacks.

Cyber-attacks are a major threat to the Smart Grid. They can be launched remotely and are designed to exploit vulnerabilities in the Smart Grid's communication and control systems. Cyber-attacks can take various forms, such as denial-of-service attacks, phishing attacks, malware attacks, and advanced persistent threats. These attacks can result in data theft, service disruption, equipment damage, and even physical harm to the operators and the public. The vulnerabilities of the Smart Grid extend to all its elements, including software, hardware, and data transfer systems. The Smart Grid relies on various software components, such as operating systems, control systems, and database management systems. These components can contain security vulnerabilities that can be exploited by attackers. Similarly, hardware components, such as routers, switches, and sensors, can also be targeted by attackers.

Moreover, the data transfer systems used by the Smart Grid, such as wired and wireless networks, can be vulnerable to attacks. These systems can be targeted by attackers who want to intercept, manipulate, or destroy the data transferred over them. Finally, the Smart Grid's operational procedures and applications, such as energy management systems and billing systems, can also be targeted by attackers who want to disrupt the grid's operations or steal confidential information. The Smart Grid is vulnerable to various system vulnerabilities and cyber-attacks.

These vulnerabilities can have serious implications for national security, economic stability, and public safety. Therefore, it is essential to develop effective detection methodologies and cybersecurity solutions to ensure the Smart Grid's security and reliability.

B. CYBER-ATTACK DETECTION TECHNIQUES

To detect cyber-attacks on the Smart Grid, various detection methodologies have been introduced in previous studies. These methodologies can be classified into three categories: signature-based, anomaly-based, and hybrid-based detection. Signature-based detection relies on predefined signatures or patterns of known cyber-attacks to identify and block malicious traffic. This approach is effective against known attacks, but it is less effective against new and unknown attacks that do not match the predefined signatures. Anomaly-based detection, on the other hand, relies on statistical analysis and machine learning algorithms to detect abnormal behavior or deviations from normal patterns in the Smart Grid's network traffic. This approach can detect unknown and zero-day attacks, but it can also generate false alarms and miss some attacks that are similar to normal behavior. Hybrid-based detection combines the strengths of signature-based and anomaly-based detection. This approach uses predefined signatures to detect known attacks and machine learning algorithms to detect unknown and abnormal behavior in the Smart Grid's network traffic. This approach can provide a higher level of accuracy and reduce false alarms.

In addition to these detection methodologies, various techniques have been proposed to enhance the detection of cyber-attacks on the Smart Grid. These techniques include deep learning, feature selection, and ensemble learning. Deep learning techniques, such as convolutional neural networks (CNNs), can automatically learn and extract features from the Smart Grid's network traffic and use them to detect cyber-attacks. These techniques can provide high accuracy and reduce false alarms. Feature selection techniques can reduce the dimensionality of the Smart Grid's network traffic and improve the performance of the detection algorithms.

These techniques can select the most relevant features that are important for detecting cyber-attacks and remove irrelevant and redundant features. Ensemble learning techniques can combine multiple detection algorithms to improve the accuracy and robustness of the detection system. These techniques can reduce the risk of false alarms and provide a higher level of confidence in the detection results. Various detection methodologies and techniques have been proposed to detect cyber-attacks on the Smart Grid. These methodologies and techniques can provide a higher level of accuracy and reduce false alarms, and they can enhance the security and reliability

of the Smart Grid. The detecting cyber-attacks in the Smart Grid would consist of several components such as:

1) Smart Grid devices and components: This includes all the devices and components of the Smart Grid such as smart meters, sensors, controllers, and communication networks.
2) Data pre-processing and feature selection: This component is responsible for pre-processing the data generated by the Smart Grid devices and selecting the most relevant features for detecting cyber-attacks.
3) Machine learning algorithms: This component includes various machine learning algorithms such as decision trees, random forests, and support vector machines that can learn patterns from the Smart Grid data and detect cyber-attacks.
4) Anomaly detection and signature-based detection: This component includes anomaly detection techniques and signature-based detection techniques that can detect abnormal behavior and known cyber-attacks in the Smart Grid data.
5) Ensemble learning: This component combines multiple detection algorithms to improve the accuracy and robustness of the detection system and reduce the risk of false alarms.
6) Intrusion detection system (IDS): This component monitors and analyzes the Smart Grid data for signs of suspicious activity and raises an alert if an attack is detected.
7) Security information and event management (SIEM) system: This component collects and analyzes data from different components of the Smart Grid and uses correlation and pattern recognition techniques to detect cyber-attacks.

Overall, the designed to integrate different detection methodologies and techniques to improve the accuracy and reliability of the cyber-attack detection system in the Smart Grid as shows respectively in Figures 5 and 6.

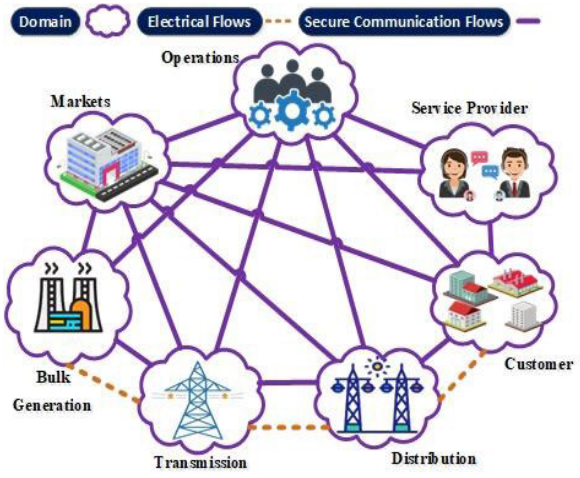

FIGURE 5. Frameworks of IoT [5].

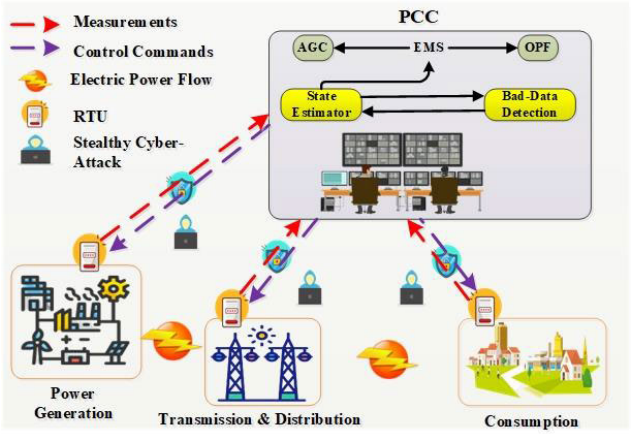

FIGURE 6. Illustration of a smart grid's conceptual model.

C. DATASETS FOR CYBER-ATTACK DETECTION

The use of relevant data sets is essential in training and assessing machine learning models specifically developed to detect and mitigate cyber-attacks. The availability of these datasets is crucial for academics and practitioners to create efficient algorithms and systems for the detection of cyber-attacks. The dimensionality of these datasets varies based on the number of characteristics or variables employed to depict network traffic. Commonly, the datasets employed for cyber-attack detection might encompass hundreds to tens of thousands of characteristics that portray distinct facets of network behavior and communication. The process of framing the issue of cyber-attack detection as a big data problem requires the management and analysis of vast quantities of data produced by network operations. This encompasses the difficulties associated with scaling, optimizing storage, and processing data with a large number of dimensions. Apache Hadoop and Apache Spark, which are big data technologies, can be employed to solve the difficulties associated with managing and analyzing massive amounts of information with the aim of detecting cyber-attacks. Following are many prominent datasets frequently utilized in the field:

1) The NSL-KDD dataset is an enhanced iteration of the extensively utilized KDD Cup 1999 dataset. It rectifies several deficiencies of the first dataset and offers a more authentic portrayal of network activity.
2) The UNSW-NB15 dataset is a collection of network traffic data specifically designed for evaluating network-based intrusion detection systems (NIDS). It encompasses a broad spectrum of both malicious assaults and regular operations within a network.
3) The CICIDS2017 dataset is a recent collection of data from the Canadian Institute for Cybersecurity that contains both harmless and harmful network traffic. Its purpose is to assess the efficacy of intrusion detection systems.
4) The dataset is called AWID (Aarhus WiFi IDS). The AWID dataset is specifically designed to analyze and address security issues related to wireless networks.

It contains data collected from a WiFi intrusion detection system. It detects several forms of assault in a wireless setting.

5) The dataset used is ISCX-IDS-2012. The origin of this dataset may be traced back to the 2012 International Cyber Security Challenge (ICSC). The controlled environment encompasses a diverse range of threats aimed at assessing the effectiveness of intrusion detection systems.
6) The KDD Cup 1999 dataset, although dated, is a widely recognized benchmark dataset that has been extensively utilized in early research on intrusion detection. It consists of a wide range of characteristics derived from network traffic.

D. DEEP LEARNING APPROACHES FOR CYBER-ATTACK DETECTION

Deep learning methods have demonstrated potential for enhancing the precision of cyberattack detection by autonomously acquiring hierarchical characteristics from unprocessed data. Here are a few pertinent methodologies:

1) Convolutional Neural Networks (CNNs): CNNs have effectively been utilized for detecting intrusions in network traffic by acquiring knowledge of spatial patterns within the data. These algorithms have the ability to perform functions such as infection detection or the recognition of unusual patterns in network traffic [123].
2) Recurrent neural networks (RNNs) are advantageous for evaluating sequential data, such as time-series logs or network packet sequences. LSTM networks, which are a form of recurrent neural network (RNN), are adept at identifying long-range associations in time-varying data [124].
3) Autoencoders: Anomaly detection may be achieved through the utilization of unsupervised learning using autoencoders. By effectively modeling standard patterns, these models may detect differences that suggest possible cyber risks [125].
4) Generative adversarial networks (GANs) may be utilized to produce artificial data for the purpose of enhancing training sets or simulating cyber-attacks. This contributes to the model's acquisition of a wide range of attack patterns [126].

Regarding the significance of classical feature selection techniques in the era of deep learning, it is significant that deep learning models are designed specifically to, without supervision, acquire appropriate characteristics from unprocessed data, frequently obviating the necessity for explicit feature engineering. Nevertheless, there are situations in which feature selection approaches can still be advantageous, particularly when working with data that has a large number of dimensions or requires domain-specific expertise.

E. PHYSICS-INFORMED MACHINE LEARNING (PIML)

Physics-Informed Machine Learning (PIML) techniques are a specific category of machine learning (ML) approaches used to identify and detect cyber-attacks [127]. The current plans and methods use the basic physical features of the power grid along with different types of machine learning, such as supervised or semi-supervised learning, unsupervised learning, and reinforcement learning (RL) [128]. The literature on PIML techniques for applications such as anomaly detection, classification, and localization. The advancement in digital automation for smart grids recently led to the use of measuring devices such as phasor measurement units (PMUs), micro-PMUs (μ-PMUs), and smart meters [127]. However, the large amount of data collected from these sensors causes many challenges since control room operators need to integrate this data with models in order to make educated decisions for the reliable and resilient operation of the cyber-power systems [129]. The ML-based solutions provide a reliable analysis of the significant quantity of data collected from the field. In order to ensure satisfactory network performance in all situations, decision-makers need to utilize technologies adept at identifying solutions that are economically acceptable and compatible with the system's limitations [130]. These appliances are efficient, reliable, and simply comprehensible. As a result, the use of PIML approaches continues to develop to solve problems using model-based or data-driven machine learning techniques [131]. Therefore, ML techniques have the ability to detect and analyze connections across distance, time, and data patterns, leading to the generation of detailed and precise solutions [132]. Furthermore, these techniques could provide results that satisfy the demands of real-time monitoring and control in the electric grid, a critical feature for ensuring dependable and effective operation [133]. Efficiently handling the significant amount of data generated by these sensors is a challenge for decision-making procedures [134]. Improving the understanding of the system's dynamics leads to a more accurate perception and increases the potential of identifying abnormal metrics, such as outliers or anomalies [135].

III. CHALLENGES

The ever-evolving nature of cyber threats poses a significant challenge to the smart grid's security. The attackers are continually developing new techniques to breach the system, making it difficult to predict and mitigate potential risks. The complexity and interconnectivity of smart grid components also make it challenging to implement security measures that cover all system elements. Additionally, the lack of standardization across the smart grid industry is a challenge in developing comprehensive security protocols that are universally adopted. Furthermore, the cost associated with implementing robust security measures in a smart grid system can be substantial, and this may hinder some stakeholders from investing in adequate security solutions. Finally, the shortage of cybersecurity professionals with the necessary expertise in smart grid security is another challenge. The increasing demand for these professionals, coupled with the

limited supply, may result in a skills gap that could leave smart grid systems vulnerable to cyber threats.

A. SMART GRID CYBER-PHYSICAL SECURITY (VULNERABILITIES)

Vulnerability can be defined as a flaw in the computational logic (such as coding) identified in hardware and software components that, when abused, causes a negative effect on secrecy, integrity, OR availability [136]. In this respect, vulnerability mitigation often entails code improvements, but it may also entail specification changes or even design vocation [136]. Recent smart grids have grown into a sophisticated technological system that combines physical networks, IT, and OT, as well as interoperates and engages with several other essential assets. All vulnerabilities [137] incorporated in the grid system, including those of external entities associated with it, have a significant effect on grid cybersecurity. Vulnerability is a big concern to smart grids and can possibly result in a variety of effects such as power failures, power dissipation, financial harm, and so on.

B. PHYSICAL COMPONENTS SECURITY

A smart grid is made up of many different elements, including equipment, software, and control systems. All of these elements are vulnerable in some way, including:

1) Weak physical access control systems, such as insufficient video surveillance and autonomous site inspection.
2) Insufficient physical protection for DERs at remote areas.
3) Internal layoff limits inside the substation.
4) Insufficient long-line surveillance.
5) Outdated parts and lengthy maintenance delays for faulty equipment.
6) Inadequate electromagnetic pulse filtering near the smart grid system.
7) Poor grid operating physical-world. These possible concerns are typical issues that arise from natural or not natural physical harm [138], and there are several established techniques and approaches of prevention available.

These physical weaknesses, on the other hand, have the ability to assist a concerted cyberattack, a mixture of local and opponent intrusions.

C. VULNERABILITIES IN IT/OT

Information technology (IT) or Operational technology (OT) advancements have enabled linked substations to function together with little or no human contact. With more new technologies being incorporated into smart grids, maintaining grid security is becoming increasingly difficult. This integration of OT and IT is altering the mindset and method to smart grid cyber-security. At the same time, all of IT/weaknesses OTs constitute a danger element to the whole grid system [138].

Smart grids are made up of a diverse set of smart software and hardware, particularly networked computers. Any weakness in this software and hardware might result in cyber-attacks [139]. The Common Vulnerability Scoring System (CVSS) and Common Vulnerabilities and Exposures (CVE) metrics demonstrate a long-term pattern of rising weaknesses in grids components and associated programs [140], [141]. ''The weakness of those devices with networking capabilities and smart operation is increasing so fast, not only due to more vulnerabilities in smart technologies, but also due to developing the systems of the smart grids, relatively new smart grid environmental elements, and inflating services and applications'' [141]. ''Data communication vulnerabilities also enable network-based attacks and other communication [142], [143].

The OT communication lacks adequate security design to secure data transmission inside OT parts and with IT parts. This is largely a smart grid vulnerability that is difficult to address in the short future. It might take a long time to replace technology and equipment and improve OT. The weakness in IT communications is not novel, but it serves as a conduit between the external attacker and the internal OT.

D. DATA MANAGEMENT SECURITY

Current data management of smart grids has issues with clustering integrity, confidentiality, compliance control, shared scope, and management method efficiency. A vast volume of data is produced and moved between many entities. Data packet streams that are accurate and consistent, including as power grid, weather predictions, and business-related information, enable operators to regulate and oversee the system of the smart grids. This sort of information is critical for avoiding unexpected and sudden power outages and maintaining the quality of grid operations and businesses. Furthermore, such huge data may be utilized for grid operations, alerts, demand forecasting, generation estimations, pricing changes, and so on. Because numerous smart grid sectors are engaged in the process, the data gathered is rather big. In addition, there is a statutory need to give correct data as often as feasible, which is difficult. Yet, several weaknesses are there in the cyber environment's long chain of information gathering, analysis, computing, security, and control [14], [144].

E. APPLICATIONS AND SERVICES SECURITY

The access to IT and OT information allows the quick physical data translation into useful information, allowing sophisticated financial advisory platforms, distribution grid technologies, and distributed energy management systems to be developed [145]. The applications have resulted in some incredible advantages for asset-rich substations. Interconnectivity speeds up data flow between devices, allowing for the automating of substation control and protection systems and giving operational advantages. Smart grids may offer a wide range of services and applications, including energy trading, electricity services, energy converging, and numerous client services.

All of these services based on digitization depend on grid operation, grid connectivity, data collecting, and the modeling of application process [145]. On the smart grid, there are various inherent weaknesses and vulnerabilities in systems of information technology programs that are significantly expanded in size and extend to all sectors of services and applications [145], [146]. All of these flaws substantially impair the routine functioning and services of smart grids. These vulnerabilities include:

1) Inadequate patching and frequent upgrades, resulting in unpatched software and systems.
2) Failures in common mode.
3) Inadequate resources management.
4) Inadequate documentation of maintenance control.
5) Using obsolete versions of Operating system (OS).
6) Inadequate grid separation from the World Wide Web.
7) Shortage of OT intrusion detection systems.
8) Inadequate OT malware identification & protection [146].

F. RUNNING ENVIRONMENT SECURITY

The operational environment of smart grids covers various layers, ranging from technologies to community, individuals, morality, economics, national policy, and the regulatory environment [146], [147]. As a result, the classic grid operating environment vulnerabilities are including a lot of non-IT aspects, such as: Staff ineptness, such as absence of specialized skills, unreliable and dishonest behavior, and so on; Noncompliance with national and global rules; Political, war, or proxy wars. The majority of the aforementioned risks should be addressed by a combination of technological and nontechnical solutions, such as increased cyber-security awareness, adequate advanced training, and regular controlling of the smart grid's complete working environment. Since the smart grids are traditional vital infrastructures, they may be particularly vulnerable to assault in difficult settings. As a result, the political and geopolitical context should not be overlooked.

G. EVOLVING AND COMPLEX SMART GRIDS SECURITY

Smart grids are developing and changing, including increasingly more IEDs and elements, connecting to multiple network systems, supporting an increasing number of applications and functions, and interfacing with other essential infrastructures. As a result, smart grids are a typical SoS. Every vulnerability in just about any component of the complicated advanced systems endangers the smart grid, and the dynamism and intricacy end up making vulnerability identification and treatment much more difficult [148], [149]. Vulnerability assessment, identification, and restoration must be handled methodically and in tandem with cyberattack evaluation. The majority of cyberattacks target smart grid system vulnerabilities, particularly those in components and networked devices. The security of Smart grid is more than just creating secure networks. A more reasonable way would be to create an effective management of networking system vulnerability that can swiftly react to changing situations while causing minimal defect to smart grids. The following are the primary duties for vulnerability management:

1) Identify as many and full vulnerabilities at all levels of the system as feasible, as each unknown vulnerability might lead to significant security issues. The security of smart grids is decided by the most vulnerable link, not the most secured one.
2) As quickly as feasible, repair or eliminate system vulnerabilities. Once vulnerabilities have been identified, hidden risks should be eradicated as soon as feasible. Many cyberattacks take use of zero-day weaknesses.
3) Association of vulnerabilities. The system's ultimate weakness is more than just a collection of weaknesses. It is vital to determine their logical, functional, and physical relationships as well as their aggregation criteria. This provides a comprehensive overview of smart grid system vulnerabilities.
4) System vulnerabilities must be discovered and analyzed automatically. The system of the smart grids has several weaknesses or vulnerabilities, and it is challenging to identify and evaluate all of them manually using thorough approaches in a timely manner. Automated techniques for vulnerability identification, analysis, and management must be created.
5) Analysis of vulnerabilities and attack matches. A 100% of the cyberattacks target single or multiple system weaknesses. In defending and safeguarding system security, a detailed vulnerabilities map and assaults is quite useful.
6) To tackle the weaknesses, a systematic approach including countermeasures is required. A single point of failure or weakest spot in a smart grid is always a difficulty.

IV. CYBER-PHYSICAL ATTACKS

Lately, there has been an increase in interest in analyzing Cyber-Physical System of Systems or group (CPSG) vulnerabilities. The usual strategy is to investigate individual attacks on a certain system component. A CPSG is made up of information and OT. IT corresponds to the use of networks to handle data and the movement of digital information. OT, on the other hand, refers to technology which controls and monitors certain equipment like the SCADA system. IT and OT are converging, a process called as IT-OT convergence, and the line between them is becoming increasingly blurred.

A. DATA AVAILABILITY ATTACKS

Opponents can launch attack methods against the channel of communication since cellular communication is widely employed in a CPSG. We classify assaults that limit accessibility as IT attacks in this study [150], [151]. These attacks are initiated by exploited interior routers to disrupt trusted routing, lowering the overall performance of the network [151]. Naturally, attackers undertake Byzantine assaults with two goals in mind. The initial goal is vandalism, in which cyber-attackers claim channel emptiness while sensing data

show that the channel is active. The 2nd goal is exploited, in which attackers get exclusive connection to the idle channel by transmitting channel busy data when their detecting findings show that the channel is idle. Attackers can maximize their attack usefulness by pursuing the aforementioned goals [152]. In contrast to Byzantine attacks, which impede availability of data by weakening the communication channel, DoS assaults obstruct regular data transit by filling the communication channel with garbage data. A DoS attack in a CPSG aims to interrupt communications between a control center and field sensors or actuators. DoS attackers do not need to understand the CPSG settings or be able to change measurement or control information in the communication channel. As a result of the loss of measurement data, system operators can readily detect the assault. However, the operators are unable to stop the onslaught since they are unable to send control signals to the actuators. The above-mentioned incident involving Ukrainian electric power providers is an example of a DoS attack [153], [154].

B. CONTROL SIGNAL ATTACKS

1) AURORA ATTACKS

The Idaho National Laboratory discovered the aurora generator vulnerability, in which a hypothetical attacker intentionally opens and closes a generator's circuit breaker by inserting a sequence of compromised control instructions [155]. When the generator is unplugged from the electrical grid, it becomes desynchronized. When the system and generator go out of sync, the aurora attack is meant to re-close the breaker before the protective system responds to the attack [156], [157]. Because generator protection parts are purposely delayed minimizing needless tripping, attackers generally have a 15-cycle window before any protection mechanism kicks in [3] and [158].

2) PRICING ATTACKS

Retail markets are paying more attention to demand-response systems in order to improve grid efficiency. In its most basic form, demand-response is a control system in which control signals serve as incentives. Tan et al. [159] developed a pricing assault on price signals by scaling and delaying. Giraldo et al. [160] ''enhanced the assault even further by simulating an attacker who intends to raise the imbalance between consumed and generated energy by infiltrating the communication channel and employing an attack time series to influence the pricing signal. Unlike one-shot attacks, in which the attackers inject harmful data just once'' [160], authors of [161] evaluated assaults capable of inserting incorrect price data at any time and frequently over a lengthy period of time. Long-term assaults can generate a power imbalance, which can result in over-generation, economic losses, and poor quality of energy. The authors devised a sensitivity analysis approach to measure the impact of repeated assaults. They used a z-transform sensitivity functionality to represent the system's dynamics in their investigation.

The authors of [162] enhanced the pricing assault by injecting fraudulent bidding quantities and prices from prosumers through malware. The market clearing price was altered as a result of these assaults, and each individual prosumer's energy usage was altered, negatively affecting total demand on distribution feeders. In [162], two attack possibilities were investigated: the first intended to undermine the system's dependability by influencing the bid price to certain extreme levels, while the second aimed at reaping profit over time by influencing the bid price within bounds to prevent detection. Prosumers are aware of these bid restrictions because of the service agreement. If the attacker distorts the impulses to the point where they exceed the restrictions, the modification will be visible [161]. In comparison to the first scenario, the assault in the second scenario has a minor influence on the total load, making detection difficult.

C. MEASUREMENT ATTACKS

1) AGC ATTACKS

In linked power grids, Automatic Generation Control (AGC) is a wide-area frequency control application. The controller error is calculated by AGC using flow of power and frequency information from distant sensors (ACE). AGC is vulnerable to measurement assaults because to the lack of a measurement verification or attack detection system. Once hacked, it has the potential to quickly generate an imbalance of power in the system. The adversary in this example is a provider that intends to produce more electricity than the assigned timetable without being noticed. Another type of attack targets power flow sensors by employing a sustained fake data injection attack across numerous AGC cycles. Chen et al. [163] investigated the 4 sorts of attacks used to accomplish the AGC attack approach, which targeted the control of load frequency explicitly.

2) FDI ATTACKS

FDI assaults on bad data detection and state prediction are two of the smart grid's hottest subjects. Liu et al. [164] were the first to show it using DC system models. They believed that the attacker is familiar with the network settings and topology of the whole power system, as well as the capacity to manipulate data readings from meters. An FDI assault has the potential to defraud the power system state estimate, which serves as the basis for a lot of functions of power system like contingencies and revenue maximization [165], [166]. Falsified state estimate findings may cause the EMS's functioning and auto-control mechanism to malfunction. Financial damage, unpredictable system states, and even system voltage failure are all possible outcomes of such attacks [167]. Authors in [168] proposed an FDI attack capable of causing physical line overflows, as shown in Figure 7. Considering the EMS sequential information computing features, their optimal attack vector caused line overload when incorrect parameters caused generation dispatch. Intricately designed cyberattacks can avoid bad data identification by adhering to physical rules such as Kirchhoff's circuit laws.

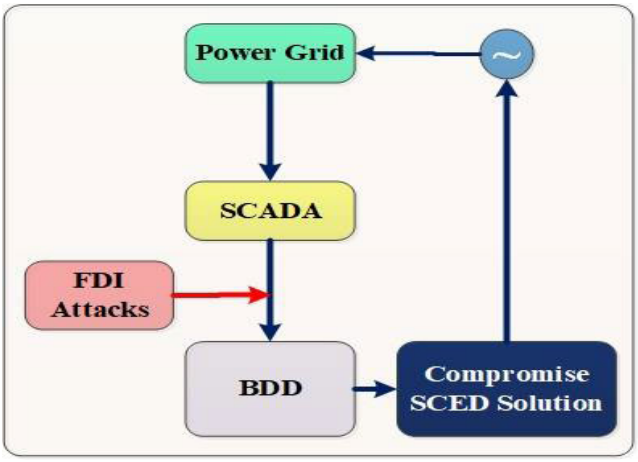

FIGURE 7. FDI assaults on economic load dispatch.

3) BLIND FDI ATTACKS

With no knowledge acquisition of the power grid structure, blind FDI threats can be built. The assault is built using the principal component analysis (PCA) [169] estimation approach. The topological data can be incorporated in the connections between measurements. While, data-driven tactics, particularly machine learning-based Apache's, are an important component of cyber-physical assaults against smart grids. If an opponent is aware of the susceptibility of all transmission lines that are proceeding to that bus, they can undertake concealed FDI assaults to manipulate the state variable on that bus. Authors in [170] developed an unsupervised learning strategy to cluster the data set in circumstances when attackers are unable to identify the eavesdropped measurement related to the existing system architecture. For dimensional reduction, the suggested data categorization uses T-distributed stochastic neighbor embedding. Despite the fact that attackers can gain topology information in the scenarios mentioned above, attackers may also construct FDI assaults with little topology knowledge [171].

a: LOAD REDISTRIBUTION

Recently, researchers have been focused on discovering the exact assault implications [172]. Che et al. [173] investigated the method by which an attacker might implicitly recognize the intended beginning uncertainty as a system weakness, then exploit such a weak spot to carry out LR assaults that result in physical harm to the system. The Security Constrained Economic Dispatch (SCED) imposes line flow limitations depending on the improper power flow status under the influence of the load attack vector. Severe transmission overloads might occur when the generators follow the dispatch directives issued by the SCED [174]. Xiang et al. [175] proposed a power system stability evaluation model to quantify the effect of LR assault on long-term power source dependability. The suggested Monte Carlo simulation-based assessment approach considers LR assaults that may result in load reduction. Fu et al. [176] introduced an attacker who coordinates LR assaults with physical attacks to target the most tripped lines throughout the cascade process rather than the most profitable lines.

b: GPS SPOOFING ATTACKS

Spoofing attacks on PMUs in CPSGs are carried out through GPS spoofing, in which the attacker generates false GPS signals [177]. The other sort of this kind of attacks is known as the time stamp assault, also known as a time synchronization attack (TSA), and it aims to intentionally insert erroneous time stamps, causing an incorrect phase angle in the PMU measurements [178]. Authors of [179] devised an optimization issue to determine the most susceptible PMUs for use in the construction of a TSA. The state estimate error was used to quantify the vulnerability, and a greedy method was used to address the issue.

D. ATTACKS ON CONTROL SIGNAL MEASUREMENT

Authors of [180] proposed two coordinated cyber-physical attacks to conceal the line outage: replaying and optimized coordinated cyber-physical attacks. The replayed coordinated cyber-physical attacks are highly expensive, and the real system state differs from the manipulation measures, making it observable by separately known-secure PMUs. The enhanced coordinated cyber-physical attacks cancel out the effect of the power loss on the BDD residue. Li et al. [181], [182] advocated two-step cyberattacks to hide line disruptions caused by physical attacks. Cyberattacks are divided into two stages, the first of which is a topology-preserving assault, followed by a load redistribution attack. An AC model is used to build the attack vector, which includes information about the local network and the capacity to change measurement inside the assaulted region [183].

V. NOVELTY

In recent years, several prospective cybersecurity approaches have been proposed for enhancing the security of smart grids against cyber-attacks. Here are some of the key approaches:

1. Artificial Intelligence (AI) and Machine Learning (ML): AI and ML techniques have been widely used for detecting and mitigating cyber-attacks in smart grids. AI and ML can analyze vast amounts of data generated by smart grids and detect patterns that may indicate a cyber-attack. Additionally, AI and ML can be used to develop advanced intrusion detection systems (IDSs) that can identify new and unknown cyber-attacks.
2. Blockchain: Blockchain technology can be used to secure smart grid transactions and data transfers. Blockchain provides a decentralized and tamper-proof ledger of transactions that can prevent unauthorized changes to data. This approach can be used to secure smart grid data transfers and ensure that only authorized users can access sensitive information.
3. Software-Defined Networking (SDN): SDN is a networking approach that separates the control and data planes of a network. SDN can be used to create dynamic and

programmable networks that can respond to cyber-attacks in real-time. Additionally, SDN can be used to isolate infected devices or networks to prevent the spread of malware.

4. Hardware Security: Hardware security techniques such as physically unclonable functions (PUFs) and trusted platform modules (TPMs) can be used to enhance the security of smart grid hardware. PUFs are hardware-based security features that can generate unique keys for each device, which can be used for authentication and encryption. TPMs are specialized chips that can store sensitive data such as encryption keys and can be used to ensure the integrity of the device.
5. Cloud Computing: Cloud computing can be used to enhance the security of smart grids by providing secure and scalable computing resources. Cloud computing can be used to store sensitive data and provide secure communication channels between devices. Additionally, cloud computing can be used to develop advanced IDSs and to perform real-time threat analysis.
6. Overall, the prospective cybersecurity approaches for smart grids involve a combination of technologies and techniques, including AI and ML, blockchain, SDN, hardware security, and cloud computing. These approaches can help to enhance the security of smart grids and prevent cyber-attacks.

VI. TECHNOLOGICAL FUTURE PROSPECTS FOR CYBER-ATTACK IN SMART GRID

The technological future prospects for cyber-attacks in the smart grid are constantly evolving as new technologies and security measures are developed. Some of the promising future prospects for enhancing smart grid cybersecurity are discussed below:

1. Artificial Intelligence (AI) - AI has the potential to improve smart grid cybersecurity by automating threat detection and response. Machine learning algorithms can be trained to recognize and classify anomalous behavior in the grid's systems, allowing for early detection of cyber-attacks.
2. Blockchain - Blockchain technology has the potential to enhance smart grid cyber-security by providing a secure and tamper-proof record of all transactions on the grid. This can help prevent unauthorized changes to the grid's systems and data.
3. Quantum computing - Quantum computing could revolutionize smart grid cyber-security by providing exponentially faster processing speeds, making it easier to analyze vast amounts of data and detect cyber-attacks in real-time.
4. Edge computing - Edge computing involves processing data closer to the source of the data, reducing latency and improving response times. This can be particularly useful in smart grid cybersecurity, where fast response times are essential to prevent cyber-attacks.
5. Internet of Things (IoT) security - The proliferation of IoT devices on the smart grid presents a significant security risk. Future cybersecurity measures will need to focus on securing these devices and ensuring they are not vulnerable to cyber-attacks.
6. Cloud security - The use of cloud computing in the smart grid can improve scalability and reduce costs, but it also presents security challenges. Future cybersecurity measures will need to focus on securing cloud infrastructure and data.
7. Threat intelligence Cyber-attack detection can be improved by integrating threat intelligence data from multiple sources, such as public and private sector organizations. This can help identify emerging threats and prevent cyber-attacks before they occur.

Overall, the technological future prospects for cyber-attacks in the smart grid are varied and evolving. As new technologies emerge and cybersecurity threats evolve, smart grid operators will need to continually adapt and implement new security measures to ensure the grid's safety and reliability.

TABLE 2. Main abbreviations.

Abbreviations	Description
AI	Artificial Intelligence
BDD	Bad Data Detection
CNN	Convolutional Neural Network
CAN	Controller Area Network
DAE	Denoising Autoencoder
DAL	Deep adversary learning
DL	Deep Learning
DML	Deep Machine Learning
DT	Decision Tree
FDI	False Data Injection
GDM	Group Data Modeler
GDM/AG	GDM with Adaptive Gain
IBL	Instance Based Learner
IGA	Improved Genetic Algorithm
LCNN	Lightweight Convolutional Neural Network
LTE	Long Term Evolution
MLP	Multilayer Perceptron
ML	Machine Learning
PMU	Phasor Measuring Unit
RBM	Restricted Boltzmann Machine
SDAE	Stacked De-noising Auto Encoder
SVM	Support Vector Machine
WBAN	Wireless Body Area Networks
WiMAX	Worldwide Interoperability for Microwave Access
ARFF	Attribute-Relation File Format

VII. CONCLUSION

Cyber-threats to the security of smart grids are a serious topic that faces several hurdles from a variety of assaults. The smart grid dangers described in this paper were di-vided into two categories: system inherent vulnerabilities and external cyberattacks. Thematic taxonomy of cyberattacks on smart grids is examined in full using cutting-edge technologies that describe their assault plan, effects, and detection methods. Furthermore, blockchain technology and AI approaches are being considered as potential solutions for cyberattacks on smart grids. Despite the fact that the aforementioned technologies reliably identify assaults on smart grids, a few issues remain, most notably phony topological in-formation,

detection of faulty data, security flaws, incorporation of big data, blockchain, and so on. Since a result, future research directions are suggested from the standpoint of developing technologies for the vigorous cyber-security of smart grids against sophisticated cyberattacks, as new attack strategies are constantly uncovered.

This paper utilized the NSLKDD datasets as a benchmark for evaluating a classifier model's effectiveness in identifying intruder attacks within the realm of IoMT. The datasets consisted of various types of attacks, including DoS attacks, probing attacks, u2R attacks, and remote to local assaults. The approach employed SML and RNN techniques, which proved to be suitable for IoMT scenarios that utilize peer-to-peer unique internet protocol addresses to connect smart medical devices. Furthermore, our research focused on strengthening the cybersecurity of existing power grids by introducing a two-stage learning-based solution. This solution combined spatial domain methods and im-age-based DL approaches to detect and identify FDIAs (False Data Injection Attacks). Initially, the issue of FDIA detection and localization was addressed as a multi-label classification task, later transitioning into an image recognition task. Through our efforts, we successfully developed a robust CNN-based multiclass classifier that outperforms state-of-the-art detectors.

REFERENCES

[1] M. Faheem, S. B. H. Shah, R. A. Butt, B. Raza, M. Anwar, M. W. Ashraf, M. A. Ngadi, and V. C. Gungor, "Smart grid communication and information technologies in the perspective of Industry 4.0: Opportunities and challenges," *Comput. Sci. Rev.*, vol. 30, pp. 1–30, Nov. 2018.

[2] M. Z. Gunduz and R. Das, "Analysis of cyber-attacks on smart grid applications," in *Proc. Int. Conf. Artif. Intell. Data Process. (IDAP)*, Sep. 2018, pp. 1–5.

[3] H. Zhang, B. Liu, and H. Wu, "Smart grid cyber-physical attack and defense: A review," *IEEE Access*, vol. 9, pp. 29641–29659, 2021.

[4] H. Rahimpour, J. Tusek, A. Abuadbba, A. Seneviratne, T. Phung, A. Musleh, and B. Liu, "Cybersecurity challenges of power transformers," 2023, *arXiv:2302.13161*.

[5] P. Aurucci, "Applications and security risks of artificial intelligence for cyber security in digital environment," in *Intelligent Environments*. IOS Press, 2018, pp. 308–317.

[6] D. Ding, Q.-L. Han, X. Ge, and J. Wang, "Secure state estimation and control of cyber-physical systems: A survey," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 1, pp. 176–190, Jan. 2021.

[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, no. 18, p. 6799, Sep. 2022.

[8] D. Faquir, N. Chouliaras, V. Sofia, K. Olga, and L. Maglaras, "Cybersecurity in smart grids, challenges and solutions," *AIMS Electron. Electr. Eng.*, vol. 5, no. 1, pp. 24–37, 2021.

[9] T. Ahmad, R. Madonski, D. Zhang, C. Huang, and A. Mujeeb, "Data-driven probabilistic machine learning in sustainable smart energy/smart energy systems: Key developments, challenges, and future research opportunities in the context of smart grid paradigm," *Renew. Sustain. Energy Rev.*, vol. 160, May 2022, Art. no. 112128.

[10] X. Yuan, P. He, Q. Zhu, and X. Li, "Adversarial examples: Attacks and defenses for deep learning," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 30, no. 9, pp. 2805–2824, Sep. 2019.

[11] Z. Zhang, Q. Liu, S. Qiu, S. Zhou, and C. Zhang, "Unknown attack detection based on zero-shot learning," *IEEE Access*, vol. 8, pp. 193981–193991, 2020.

[12] L. Zhou, X. Ouyang, H. Ying, L. Han, Y. Cheng, and T. Zhang, "Cyber-attack classification in smart grid via deep neural network," in *Proc. 2nd Int. Conf. Comput. Sci. Appl. Eng.*, Oct. 2018, pp. 1–5.

[13] X. Ma, J. Wu, S. Xue, J. Yang, C. Zhou, Q. Z. Sheng, H. Xiong, and L. Akoglu, "A comprehensive survey on graph anomaly detection with deep learning," *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 12, pp. 12012–12038, Dec. 2023.

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

[15] A. Gumaei, M. M. Hassan, S. Huda, M. R. Hassan, D. Camacho, J. Del Ser, and G. Fortino, "A robust cyberattack detection approach using optimal features of SCADA power systems in smart grids," *Appl. Soft Comput.*, vol. 96, Nov. 2020, Art. no. 106658.

[16] Y. Zhang, L. Wang, W. Sun, R. C. Green II, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 796–808, Dec. 2011.

[17] T. Berghout, M. Benbouzid, and S. M. Muyeen, "Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects," *Int. J. Crit. Infrastructure Protection*, vol. 38, Sep. 2022, Art. no. 100547.

[18] J. Verbraeken, M. Wolting, J. Katzy, J. Kloppenburg, T. Verbelen, and J. S. Rellermeyer, "A survey on distributed machine learning," *ACM Comput. Surv.*, vol. 53, no. 2, pp. 1–33, 2020.

[19] T. Zheng, M. Liu, D. Puthal, P. Yi, Y. Wu, and X. He, "Smart grid: Cyber attacks, critical defense approaches, and digital twin," 2022, *arXiv:2205.11783*.

[20] O. G. M. Khan, A. Youssef, E. El-Saadany, and M. Salama, "LSTM-based approach to detect cyber attacks on market-based congestion management methods," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2021, pp. 1–5.

[21] A. Al-Abassi, J. Sakhnini, and H. Karimipour, "Unsupervised stacked autoencoders for anomaly detection on smart cyber-physical grids," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, 2020, pp. 3123–3129.

[22] M. T. Hagan, H. B. Demuth, and M. Beale, *Neural Network Design*. PWS, 1997.

[23] G. Hinton, L. Deng, D. Yu, G. E. Dahl, A.-R. Mohamed, N. Jaitly, A. Senior, V. Vanhoucke, P. Nguyen, T. N. Sainath, and B. Kingsbury, "Deep neural networks for acoustic modeling in speech recognition: The shared views of four research groups," *IEEE Signal Process. Mag.*, vol. 29, no. 6, pp. 82–97, Nov. 2012.

[24] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 7553.

[25] M. B. Mollah, J. Zhao, D. Niyato, K.-Y. Lam, X. Zhang, A. M. Y. M. Ghias, L. H. Koh, and L. Yang, "Blockchain for future smart grid: A comprehensive survey," *IEEE Internet Things J.*, vol. 8, no. 1, pp. 18–43, Jan. 2021.

[26] J. Sakhnini, H. Karimipour, and A. Dehghantanha, "Smart grid cyber attacks detection using supervised learning and heuristic feature selection," in *Proc. IEEE 7th Int. Conf. Smart Energy Grid Eng. (SEGE)*, Mar. 2019, pp. 108–112.

[27] M. J. Case, B. G. Johnson, K. J. Bartowitz, and T. W. Hudiburg, "Forests of the future: Climate change impacts and implications for carbon storage in the Pacific Northwest, USA," *Forest Ecology Manag.*, vol. 482, Feb. 2021, Art. no. 118886.

[28] J.-Q. Ruan, H.-Z. Wang, Y.-T. Liu, S. Aziz, J.-C. Peng, and G.-B. Wang, "AC sparse modeling for false data injection attack on smart gird," in *Proc. Asian Conf. Energy, Power Transp. Electrific. (ACEPT)*, 2017, pp. 1–5.

[29] O. M. Butt, M. Zulqarnain, and T. M. Butt, "Recent advancement in smart grid technology: Future prospects in the electrical power network," *Ain Shams Eng. J.*, vol. 12, no. 1, pp. 687–695, Mar. 2021.

[30] M. Sami, S. Q. Khan, M. Khurram, M. U. Farooq, R. Anjum, S. Aziz, R. Qureshi, and F. Sadak, "A deep learning-based sensor modeling for smart irrigation system," *Agronomy*, vol. 12, no. 1, p. 212, Jan. 2022.

[31] H. Wang, R. Cai, B. Zhou, S. Aziz, B. Qin, N. Voropai, L. Gan, and E. Barakhtenko, "Solar irradiance forecasting based on direct explainable neural network," *Energy Convers. Manage.*, vol. 226, Dec. 2020, Art. no. 113487.

[32] J. Wu, S. A. Haider, M. Irshad, J. Arshad, S. M. Noman, and A. Murthy, "Li-Pos: A light positioning framework leveraging OFDM for visible light communication," *Sensors*, vol. 21, no. 13, p. 4310, Jun. 2021.

[33] M. F. Moghadam, A. Mohajerzdeh, H. Karimipour, H. Chitsaz, R. Karimi, and B. Molavi, "A privacy protection key agreement protocol based on ECC for smart grid," in *Handbook of Big Data Privacy*, 2020 pp. 63–76.

[34] S. Aziz, M. T. Faiz, A. M. Adeniyi, K.-H. Loo, K. N. Hasan, L. Xu, and M. Irshad, "Anomaly detection in the Internet of Vehicular networks using explainable neural networks (xNN)," *Mathematics*, vol. 10, no. 8, p. 1267, Apr. 2022.

[35] A. Chehri, I. Fofana, and X. Yang, "Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence," *Sustainability*, vol. 13, no. 6, p. 3196, Mar. 2021.

[36] Z. Ma, S. Guo, G. Xu, and S. Aziz, "Meta learning-based hybrid ensemble approach for short-term wind speed forecasting," *IEEE Access*, vol. 8, pp. 172859–172868, 2020.

[37] A. Murthy, M. Irshad, S. M. Noman, X. Tang, B. Hu, S. Chen, and G. Khader, "Internet of Things, a vision of digital twins and case studies," in *IoT and Spacecraft Informatics*. Amsterdam, The Netherlands: Elsevier, 2022, pp. 101–127.

[38] B. Hu, S. M. Noman, M. Irshad, X. Tang, C. Song, and M. U. Muhammad, "Run-time prediction practices of multimedia web design in technology management," in *3D Imaging Technologies—Multidimensional Signal Processing and Deep Learning*, vol. 2. Berlin, Germany: Springer, 2021, pp. 179–186.

[39] L. Tan, Z. Tong, Z. Kaifang, Z. Liang, and Z. Li, "Fault division method of multi-infeed HVDC tranmission system based on fault current limiting technology," in *Proc. Chin. Autom. Congr. (CAC)*, Oct. 2017, pp. 5668–5672.

[40] Y. Li, W. Xue, T. Wu, H. Wang, B. Zhou, S. Aziz, and Y. He, "Intrusion detection of cyber physical energy system based on multivariate ensemble classification," *Energy*, vol. 218, Mar. 2021, Art. no. 119505.

[41] A. Shahid, "Cyber-physical modeling and control of smart grids—A new paradigm," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Sep. 2016, pp. 1–5.

[42] S. Manimurugan, S. Al-Mutairi, M. M. Aborokbah, N. Chilamkurti, S. Ganesan, and R. Patan, "Effective attack detection in Internet of Medical Things smart environment using a deep belief neural network," *IEEE Access*, vol. 8, pp. 77396–77404, 2020.

[43] M. Usman, M. A. Jan, X. He, and J. Chen, "P2DCA: A privacy-preserving-based data collection and analysis framework for IoMT applications," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 6, pp. 1222–1230, Jun. 2019.

[44] S. M. Kasongo and Y. Sun, "A deep learning method with filter based feature engineering for wireless intrusion detection system," *IEEE Access*, vol. 7, pp. 38597–38607, 2019.

[45] G. Thamilarasu, A. Odesile, and A. Hoang, "An intrusion detection system for Internet of Medical Things," *IEEE Access*, vol. 8, pp. 181560–181576, 2020.

[46] F. A. Khan, A. Gumaei, A. Derhab, and A. Hussain, "A novel two-stage deep learning model for efficient network intrusion detection," *IEEE Access*, vol. 7, pp. 30373–30385, 2019.

[47] A. Bengag, O. Moussaoui, and M. Moussaoui, "A new IDS for detecting jamming attacks in WBAN," in *Proc. 3rd Int. Conf. Intell. Comput. Data Sci. (ICDS)*, Oct. 2019, pp. 1–5.

[48] Y. Yang, K. Zheng, C. Wu, and Y. Yang, "Improving the classification effectiveness of intrusion detection by using improved conditional variational AutoEncoder and deep neural network," *Sensors*, vol. 19, no. 11, p. 2528, Jun. 2019.

[49] A. Wahid, D. M. Khan, N. Iqbal, S. A. Khan, A. Ali, M. Khan, and Z. Khan, "Feature selection and classification for gene expression data using novel correlation based overlapping score method via Chou's 5-steps rule," *Chemometric Intell. Lab. Syst.*, vol. 199, Apr. 2020, Art. no. 103958.

[50] K. Wang, L. Liu, C. Yuan, and Z. Wang, "Software defect prediction model based on LASSO–SVM," *Neural Comput. Appl.*, vol. 33, no. 14, pp. 8249–8259, Jul. 2021.

[51] S. Waghmare, F. Kazi, and N. Singh, "Data driven approach to attack detection in a cyber-physical smart grid system," in *Proc. Indian Control Conf. (ICC)*, Jan. 2017, pp. 271–276.

[52] M. R. Camana Acosta, S. Ahmed, C. E. Garcia, and I. Koo, "Extremely randomized trees-based scheme for stealthy cyber-attack detection in smart grid networks," *IEEE Access*, vol. 8, pp. 19921–19933, 2020.

[53] Y. Dai and P. Zhao, "A hybrid load forecasting model based on support vector machine with intelligent methods for feature selection and parameter optimization," *Appl. Energy*, vol. 279, Dec. 2020, Art. no. 115332.

[54] A. Naz, M. Javed, N. Javaid, T. Saba, M. Alhussein, and K. Aurangzeb, "Short-term electric load and price forecasting using enhanced extreme learning machine optimization in smart grids," *Energies*, vol. 12, no. 5, p. 866, Mar. 2019.

[55] S. Khan, K. Kifayat, A. K. Bashir, A. Gurtov, and M. Hassan, "Intelligent intrusion detection system in smart grid using computational intelligence and machine learning," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 6, p. e4062, Jun. 2021.

[56] S. H. Majidi, S. Hadayeghparast, and H. Karimipour, "FDI attack detection using extra trees algorithm and deep learning algorithm-autoencoder in smart grid," *Int. J. Crit. Infrastruct. Protection*, vol. 37, Jul. 2022, Art. no. 100508.

[57] O. Samuel, F. A. Alzahrani, R. J. U. H. Khan, H. Farooq, M. Shafiq, M. K. Afzal, and N. Javaid, "Towards modified entropy mutual information feature selection to forecast medium-term load using a deep learning model in smart homes," *Entropy*, vol. 22, no. 1, p. 68, Jan. 2020.

[58] F. Shehzad, N. Javaid, S. Aslam, and M. U. Javed, "Electricity theft detection using big data and genetic algorithm in electric power systems," *Electric Power Syst. Res.*, vol. 209, Aug. 2022, Art. no. 107975.

[59] H. Zhang, X. Yu, P. Ren, C. Luo, and G. Min, "Deep adversarial learning in intrusion detection: A data augmentation enhanced framework," 2019, *arXiv:1901.07949*.

[60] Z. Deng, Y. Lu, K. K. Wei, and J. Zhang, "Understanding customer satisfaction and loyalty: An empirical study of mobile instant messages in China," *Int. J. Inf. Manag.*, vol. 30, no. 4, pp. 289–300, Aug. 2010.

[61] J. Ren, J. Guo, W. Qian, H. Yuan, X. Hao, and H. Jingjing, "Building an effective intrusion detection system by using hybrid data optimization based on machine learning algorithms," *Secur. Commun. Netw.*, vol. 2019, pp. 1–11, Jun. 2019.

[62] J. Zhang, F. Li, H. Zhang, R. Li, and Y. Li, "Intrusion detection system using deep learning for in-vehicle security," *Ad Hoc Netw.*, vol. 95, Dec. 2019, Art. no. 101974.

[63] P. Polityuk, O. Vukmanovic, and S. Jewkes, *Ukraine's Power Outage Was a Cyber Attack: Ukrenergo*. London, U.K.: Reuters, 2017.

[64] R. A. Abouhogail and M. S. Gadelrab, "A new secure and privacy preserved protocol for IEEE802. 11s networks," *Comput. Secur.*, vol. 77, pp. 745–755, Aug. 2018.

[65] A. Derhab, M. Guerroumi, A. Gumaei, L. Maglaras, M. A. Ferrag, M. Mukherjee, and F. A. Khan, "Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security," *Sensors*, vol. 19, no. 14, p. 3119, Jul. 2019.

[66] Y. Hu, A. Yang, H. Li, Y. Sun, and L. Sun, "A survey of intrusion detection on industrial control systems," *Int. J. Distrib. Sensor Netw.*, vol. 14, no. 8, Aug. 2018, Art. no. 155014771879461.

[67] B. Appasani and D. K. Mohanta, "A review on synchrophasor communication system: Communication technologies, standards and applications," *Protection Control Modern Power Syst.*, vol. 3, no. 1, pp. 1–17, Dec. 2018.

[68] A. Khalili, A. Sami, A. Khozaei, and S. Pouresmaeeli, "SIDS: State-based intrusion detection for stage-based cyber physical systems," *Int. J. Crit. Infrastruct. Protection*, vol. 22, pp. 113–124, Sep. 2018.

[69] F. Zhang, H. A. D. E. Kodituwakku, J. W. Hines, and J. Coble, "Multilayer data-driven cyber-attack detection system for industrial control systems based on network, system, and process data," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4362–4369, Jul. 2019.

[70] W. Wang, Y. Xie, L. Ren, X. Zhu, R. Chang, and Q. Yin, "Detection of data injection attack in industrial control system using long short term memory recurrent neural network," in *Proc. 13th IEEE Conf. Ind. Electron. Appl. (ICIEA)*, May 2018, pp. 2710–2715.

[71] I. A. Khan, D. Pi, Z. U. Khan, Y. Hussain, and A. Nawaz, "HML-IDS: A hybrid-multilevel anomaly prediction approach for intrusion detection in SCADA systems," *IEEE Access*, vol. 7, pp. 89507–89521, 2019.

[72] A. Robles-Durazno, N. Moradpoor, J. McWhinnie, and G. Russell, "A supervised energy monitoring-based machine learning approach for anomaly detection in a clean water supply system," in *Proc. Int. Conf. Cyber Secur. Protection Digit. Services*, 2018, pp. 1–8.

[73] X. He, L. Zhang, T. Liu, and W. Wang, "Detecting anomalies in distributed control systems by modeling traffic behaviors," in *Proc. IEEE 4th Int. Conf. Comput. Commun. (ICCC)*, Dec. 2018, pp. 534–538.

[74] B. Zhu and S. Sastry, "SCADA-specific intrusion detection/prevention systems: A survey and taxonomy," in *Proc. 1st Workshop Secure Control Syst. (SCS)*, vol. 11, 2010, p. 7.

[75] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Comput. Surv.*, vol. 46, no. 4, pp. 1–29, Apr. 2014.

[76] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 8, pp. 1773–1786, Aug. 2016.

[77] T. Ishizaki, M. Koike, and J.-I. Imura, "Transient response improvement for interconnected linear systems: A low-dimensional controller retrofit approach," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 4, pp. 1796–1808, Dec. 2018.

[78] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1644–1652, Sep. 2017.

[79] J. Wei and G. J. Mendis, "A deep learning-based cyber-physical strategy to mitigate false data injection attack in smart grids," in *Proc. Joint Workshop Cyber-Physical Secur. Resilience Smart Grids*, 2016, pp. 1–6.

[80] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2505–2516, Sep. 2017.

[81] X. Ouyang and Z. Ma, "Using LSTM networks to identify false data of smart terminals in the smart grid," in *Proc. IEEE 23rd Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Dec. 2017, pp. 765–768.

[82] A. Sargolzaei, K. Yazdani, A. Abbaspour, C. D. Crane III, and W. E. Dixon, "Detection and mitigation of false data injection attacks in networked control systems," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4281–4292, Jun. 2020.

[83] H. Al-Sahaf, Y. Bi, Q. Chen, A. Lensen, Y. Mei, Y. Sun, B. Tran, B. Xue, and M. Zhang, "A survey on evolutionary machine learning," *J. Roy. Soc. New Zealand*, vol. 49, no. 2, pp. 205–228, 2019.

[84] D. Wilson, Y. Tang, J. Yan, and Z. Lu, "Deep learning-aided cyber-attack detection in power transmission systems," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Aug. 2018, pp. 1–5.

[85] W. Yang, M. Wang, S. Aziz, and A. Y. Kharal, "Magnitude-reshaping strategy for harmonic suppression of VSG-based inverter under weak grid," *IEEE Access*, vol. 8, pp. 184399–184413, 2020.

[86] M. Irshad, W. Liu, L. Wang, and M. U. R. Khalil, "Cogent machine learning algorithm for indoor and underwater localization using visible light spectrum," *Wireless Pers. Commun.*, vol. 116, no. 2, pp. 993–1008, Jan. 2021.

[87] Z. Qu, Y. Dong, N. Qu, H. Li, M. Cui, X. Bo, Y. Wu, and S. Mugemanyi, "False data injection attack detection in power systems based on cyber-physical attack genes," *Frontiers Energy Res.*, vol. 9, Mar. 2021, Art. no. 644489.

[88] R. Ge, G. Feng, X. Jing, R. Zhang, P. Wang, and Q. Wu, "EnACP: An ensemble learning model for identification of anticancer peptides," *Frontiers Genet.*, vol. 11, p. 760, Jul. 2020.

[89] C. Lee, P. Panda, G. Srinivasan, and K. Roy, "Training deep spiking convolutional neural networks with STDP-based unsupervised pre-training followed by supervised fine-tuning," *Frontiers Neurosci.*, vol. 12, p. 435, Aug. 2018.

[90] J. A. Boudreaux, *Design, Simulation, and Construction of an IEEE 14-Bus Power System*. Louisiana State Univ. Agricultural & Mechanical College, 2018.

[91] J. Rosen and B. Hannaford, "Doc at a distance," *IEEE Spectr.*, vol. 43, no. 10, pp. 34–39, Oct. 2006.

[92] K. K. Patel, S. M. Patel, and P. Scholar, "Internet of Things-IoT: Definition, characteristics, architecture, enabling technologies, application & future challenges," *Int. J. Eng. Sci. Comput.*, vol. 6, no. 5, 2016.

[93] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for Internet of Things (IoT) security," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1646–1685, 3rd Quart., 2020.

[94] S. Krishnan, A. Neyaz, and Q. Liu, "IoT network attack detection using supervised machine learning," Tech. Rep., 2021.

[95] X. Fu, "Statistical machine learning model for capacitor planning considering uncertainties in photovoltaic power," *Protection Control Modern Power Syst.*, vol. 7, no. 1, p. 5, Dec. 2022.

[96] Y. Huang, T. He, N. R. Chaudhuri, and T. F. L. Porta, "Preventing outages under coordinated cyber-physical attack with secured PMUs," *IEEE Trans. Smart Grid*, vol. 13, no. 4, pp. 3160–3173, Jul. 2022.

[97] T. A. Alexopoulos, G. N. Korres, and N. M. Manousakis, "Complementarity reformulations for false data injection attacks on PMU-only state estimation," *Electric Power Syst. Res.*, vol. 189, Dec. 2020, Art. no. 106796.

[98] Y. D. Mamuya, Y.-D. Lee, J.-W. Shen, M. Shafiullah, and C.-C. Kuo, "Application of machine learning for fault classification and location in a radial distribution grid," *Appl. Sci.*, vol. 10, no. 14, p. 4965, Jul. 2020.

[99] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, Jun. 2011.

[100] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Sparse attack construction and state estimation in the smart grid: Centralized and distributed models," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1306–1318, Jul. 2013.

[101] P.-Y. Chen, S. Yang, J. A. McCann, J. Lin, and X. Yang, "Detection of false data injection attacks in smart-grid systems," *IEEE Commun. Mag.*, vol. 53, no. 2, pp. 206–213, Feb. 2015.

[102] D. B. Rawat and C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Process. Lett.*, vol. 22, no. 10, pp. 1652–1656, Oct. 2015.

[103] Y. Huang, J. Tang, Y. Cheng, H. Li, K. A. Campbell, and Z. Han, "Real-time detection of false data injection in smart grid networks: An adaptive CUSUM method and analysis," *IEEE Syst. J.*, vol. 10, no. 2, pp. 532–543, Jun. 2016.

[104] V. K. Singh and M. Govindarasu, "Decision tree based anomaly detection for remedial action scheme in smart grid using PMU data," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Aug. 2018, pp. 1–5.

[105] D. Wang, X. Wang, Y. Zhang, and L. Jin, "Detection of power grid disturbances and cyber-attacks based on machine learning," *J. Inf. Secur. Appl.*, vol. 46, pp. 42–52, Jun. 2019.

[106] S. Ahmed, Y. Lee, S.-H. Hyun, and I. Koo, "Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 10, pp. 2765–2777, Oct. 2019.

[107] L. A. Maglaras and J. Jiang, "Intrusion detection in SCADA systems using machine learning techniques," in *Proc. Sci. Inf. Conf.*, 2014, pp. 626–631.

[108] L. Rajesh and P. Satyanarayana, "Detection and blocking of replay, false command, and false access injection commands in SCADA systems with modbus protocol," *Secur. Commun. Netw.*, vol. 2021, pp. 1–15, Sep. 2021.

[109] L. A. Maglaras and J. Jiang, "OCSVM model combined with k-means recursive clustering for intrusion detection in SCADA systems," in *Proc. 10th Int. Conf. Heterogeneous Netw. Quality, Rel., Secur. Robustness*, 2014, pp. 133–134.

[110] S. Salcedo-Sanz, L. Cornejo-Bueno, L. Prieto, D. Paredes, and R. García-Herrera, "Feature selection in machine learning prediction systems for renewable energy applications," *Renew. Sustain. Energy Rev.*, vol. 90, pp. 728–741, Jul. 2018.

[111] L. Cuadra, M. Pino, J. Nieto-Borge, and S. Salcedo-Sanz, "Optimizing the structure of distribution smart grids with renewable generation against abnormal conditions: A complex networks approach with evolutionary algorithms," *Energies*, vol. 10, no. 8, p. 1097, Jul. 2017.

[112] Y. Al-Smadi, M. Eshtay, A. Al-Qerem, S. Nashwan, O. Ouda, and A. A. A. El-Aziz, "Reliable prediction of software defects using Shapley interpretable machine learning models," *Egyptian Informat. J.*, vol. 24, no. 3, Sep. 2023, Art. no. 100386.

[113] C. Xu, Z. Liao, C. Li, X. Zhou, and R. Xie, "Review on interpretable machine learning in smart grid," *Energies*, vol. 15, no. 12, p. 4427, Jun. 2022.

[114] J. Li, K. Cheng, S. Wang, F. Morstatter, R. P. Trevino, J. Tang, and H. Liu, "Feature selection: A data perspective," *ACM Comput. Surv.*, vol. 50, no. 6, pp. 1–45, 2017.

[115] M. Sarhan, S. Layeghy, N. Moustafa, M. Gallagher, and M. Portmann, "Feature extraction for machine learning-based intrusion detection in IoT networks," *Digit. Commun. Netw.*, Sep. 2022.

[116] M. R. Islam, A. A. Lima, S. C. Das, M. F. Mridha, A. R. Prodeep, and Y. Watanobe, "A comprehensive survey on the process, methods, evaluation, and challenges of feature selection," *IEEE Access*, vol. 10, pp. 99595–99632, 2022.

[117] F. Anowar, S. Sadaoui, and B. Selim, "Conceptual and empirical comparison of dimensionality reduction algorithms (PCA, KPCA, LDA, MDS, SVD, LLE, ISOMAP, LE, ICA, t-SNE)," *Comput. Sci. Rev.*, vol. 40, May 2021, Art. no. 100378.

[118] K. Eckelt, A. Hinterreiter, P. Adelberger, C. Walchshofer, V. Dhanoa, C. Humer, M. Heckmann, C. Steinparz, and M. Streit, "Visual exploration of relationships and structure in low-dimensional embeddings," *IEEE Trans. Vis. Comput. Graphics*, vol. 29, no. 7, pp. 3312–3326, Jul. 2023.

[119] Y. N. Kunang, S. Nurmaini, D. Stiawan, and A. Zarkasi, "Automatic features extraction using autoencoder in intrusion detection system," in *Proc. Int. Conf. Electr. Eng. Comput. Sci. (ICECOS)*, Oct. 2018, pp. 219–224.

[120] A. T. Abed, M. S. Jit Singh, V. Thiruchelvam, S. Duraikannan, O. A. Tawfeeq, B. A. Tawfeeq, and M. T. Islam, "Challenges and limits of fractal and slot antennas for WLAN, LTE, ISM, and 5G communication: A review paper," *Ann. Telecommun.*, vol. 76, nos. 9–10, pp. 547–557, Oct. 2021.

[121] M. Mohammadpourfard, I. Genc, S. Lakshminarayana, and C. Konstantinou, "Attack detection and localization in smart grid with image-based deep learning," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Oct. 2021, pp. 121–126.

[122] S. Aziz, M. Irshad, S. A. Haider, J. Wu, D. N. Deng, and S. Ahmad, "Protection of a smart grid with the detection of cyber- malware attacks using efficient and novel machine learning models," *Frontiers Energy Res.*, vol. 10, p. 1102, Aug. 2022.

[123] S. Ho, S. A. Jufout, K. Dajani, and M. Mozumdar, "A novel intrusion detection model for detecting known and innovative cyberattacks using convolutional neural network," *IEEE Open J. Comput. Soc.*, vol. 2, pp. 14–25, 2021.

[124] W.-C. Hong, D.-R. Huang, C.-L. Chen, and J.-S. Lee, "Towards accurate and efficient classification of power system contingencies and cyber-attacks using recurrent neural networks," *IEEE Access*, vol. 8, pp. 123297–123309, 2020.

[125] A. Takiddin, M. Ismail, U. Zafar, and E. Serpedin, "Deep autoencoder-based anomaly detection of electricity theft cyberattacks in smart grids," *IEEE Syst. J.*, vol. 16, no. 3, pp. 4106–4117, Sep. 2022.

[126] N. Peppes, T. Alexakis, K. Demestichas, and E. Adamopoulou, "A comparison study of generative adversarial network architectures for malicious cyber-attack data generation," *Appl. Sci.*, vol. 13, no. 12, p. 7106, Jun. 2023.

[127] M. J. Zideh, P. Chatterjee, and A. K. Srivastava, "Physics-informed machine learning for data anomaly detection, classification, localization, and mitigation: A review, challenges, and path forward," *IEEE Access*, vol. 12, pp. 4597–4617, 2024.

[128] M. Mohammadi and A. Al-Fuqaha, "Enabling cognitive smart cities using big data and machine learning: Approaches and challenges," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 94–101, Feb. 2018.

[129] M. Chamana, R. Bhatta, K. Schmitt, R. Shrestha, and S. Bayne, "An integrated testbed for power system cyber-physical operations training," *Appl. Sci.*, vol. 13, no. 16, p. 9451, Aug. 2023.

[130] T. R. Rao, P. Mitra, R. Bhatt, and A. Goswami, "The big data system, components, tools, and technologies: A survey," *Knowl. Inf. Syst.*, vol. 60, no. 3, pp. 1165–1245, Sep. 2019.

[131] Y. Zhou, L. Xue, Z. Shi, L. Wu, and J. Fan, "Measuring housing vitality from multi-source big data and machine learning," *J. Amer. Stat. Assoc.*, vol. 117, no. 539, pp. 1045–1059, Jul. 2022.

[132] L. Zhou, S. Pan, J. Wang, and A. V. Vasilakos, "Machine learning on big data: Opportunities and challenges," *Neurocomputing*, vol. 237, pp. 350–361, May 2017.

[133] Z. Shi, W. Yao, Z. Li, L. Zeng, Y. Zhao, R. Zhang, Y. Tang, and J. Wen, "Artificial intelligence techniques for stability analysis and control in smart grids: Methodologies, applications, challenges and future directions," *Appl. Energy*, vol. 278, Nov. 2020, Art. no. 115733.

[134] X. Liu, S. Tamminen, X. Su, P. Siirtola, J. Röning, J. Riekki, J. Kiljander, and J.-P. Soininen, "Enhancing veracity of IoT generated big data in decision making," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2018, pp. 149–154.

[135] L. Erhan, M. Ndubuaku, M. Di Mauro, W. Song, M. Chen, G. Fortino, O. Bagdasar, and A. Liotta, "Smart anomaly detection in sensor systems: A multi-perspective review," *Inf. Fusion*, vol. 67, pp. 64–79, Mar. 2021.

[136] NIST. (2020). *National Vulnerability Database*. National Institute of Standards and Technology (NIST). Accessed: Feb. 3, 2021. [Online]. Available: https://nvd.nist.gov/general

[137] P. Anand, Y. Singh, A. Selwal, P. K. Singh, R. A. Felseghi, and M. S. Raboaca, "IoVT: Internet of Vulnerable Things? Threat architecture, attack surfaces, and vulnerabilities in Internet of Things and its applications towards smart grids," *Energies*, vol. 13, no. 18, p. 4813, Sep. 2020.

[138] J. Xie, A. Stefanov, and C. C. Liu, "Physical and cybersecurity in a smart grid environment," in *Advances in Energy Systems: The Large Scale Renewable Energy Integration Challenge*, 2019, pp. 85–109.

[139] C.-M. Mathas, C. Vassilakis, N. Kolokotronis, C. C. Zarakovitis, and M.-A. Kourtis, "On the design of IoT security: Analysis of software vulnerabilities for smart grids," *Energies*, vol. 14, no. 10, p. 2818, May 2021.

[140] A. Kronser, "Common vulnerabilities and exposures: Analyzing the development of computer security threats," Tech. Rep., 2020.

[141] P. Mell, J. Spring, D. Dugal, S. Ananthakrishna, F. Casotto, T. Fridley, C. Ganas, A. Kundu, P. Nordwall, V. Pushpanathan, and D. Sommerfeld, "Measuring the common vulnerability scoring system base score equation," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep., 2022.

[142] J. Lázaro, A. Astarloa, M. Rodríguez, U. Bidarte, and J. Jiménez, "A survey on vulnerabilities and countermeasures in the communications of the smart grid," *Electronics*, vol. 10, no. 16, p. 1881, Aug. 2021.

[143] Y. Xu, Y. Yang, T. Li, J. Ju, and Q. Wang, "Review on cyber vulnerabilities of communication protocols in industrial control systems," in *Proc. IEEE Conf. Energy Internet Energy Syst. Integr.*, Nov. 2017, pp. 1–6.

[144] S. Tufail, I. Parvez, S. Batool, and A. Sarwat, "A survey on cybersecurity challenges, detection, and mitigation techniques for the smart grid," *Energies*, vol. 14, no. 18, p. 5894, Sep. 2021.

[145] M. Shrestha, C. Johansen, J. Noll, and D. Roverso, "A methodology for security classification applied to smart grid infrastructures," *Int. J. Crit. Infrastruct. Protection*, vol. 28, Mar. 2020, Art. no. 100342.

[146] I. Friedberg, R. Griffin, and P. Murdock, "Smart grid security standards recommendations," Tech. Rep.

[147] T. Krause, R. Ernst, B. Klaer, I. Hacker, and M. Henze, "Cybersecurity in power grids: Challenges and opportunities," *Sensors*, vol. 21, no. 18, p. 6225, Sep. 2021.

[148] M. Alonso, J. Turanzas, H. Amaris, and A. T. Ledo, "Cyber-physical vulnerability assessment in smart grids based on multilayer complex networks," *Sensors*, vol. 21, no. 17, p. 5826, Aug. 2021.

[149] S. Borenius, P. Gopalakrishnan, L. Bertling Tjernberg, and R. Kantola, "Expert-guided security risk assessment of evolving power grids," *Energies*, vol. 15, no. 9, p. 3237, Apr. 2022.

[150] L. Zhang, G. Ding, Q. Wu, Y. Zou, Z. Han, and J. Wang, "Byzantine attack and defense in cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1342–1363, 3rd Quart., 2015.

[151] A. Geetha and N. Sreenath, "Byzantine attacks and its security measures in mobile adhoc networks," *Int. J. Comput., Commun. Instrum. Eng.*, vol. 3, no. 1, pp. 42–47, 2016.

[152] G. Ding, J. Wang, Q. Wu, L. Zhang, Y. Zou, Y.-D. Yao, and Y. Chen, "Robust spectrum sensing with crowd sensors," *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3129–3143, Sep. 2014.

[153] J. Qin, M. Li, L. Shi, and X. Yu, "Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks," *IEEE Trans. Autom. Control*, vol. 63, no. 6, pp. 1648–1663, Jun. 2018.

[154] H. Zhang and W. X. Zheng, "Denial-of-service power dispatch against linear quadratic control via a fading channel," *IEEE Trans. Autom. Control*, vol. 63, no. 9, pp. 3032–3039, Sep. 2018.

[155] M. Zeller, "Common questions and answers addressing the Aurora vulnerability," in *Proc. DistribuTECH Conf.*, 2011.

[156] *IEEE Standard for Salient-Pole 50 Hz and 60 Hz Synchronous Generators and Generator/Motors for Hydraulic Turbine Applications Rated 5 MVA and Above*, Standard 12, 2005.

[157] 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.

[158] *IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources With Associated Electric Power Systems Interfaces*, Standard 1547, 2018.

[159] R. Tan, V. Badrinath Krishna, D. K. Y. Yau, and Z. Kalbarczyk, "Impact of integrity attacks on real-time pricing in smart grids," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2013, pp. 439–450.

[160] J. Giraldo, A. Cárdenas, and N. Quijano, "Integrity attacks on real-time pricing in smart grids: Impact and countermeasures," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2249–2257, Sep. 2017.

[161] S. Maharjan, Q. Zhu, Y. Zhang, S. Gjessing, and T. Basar, "Dependable demand response management in the smart grid: A Stackelberg game approach," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 120–132, Mar. 2013.

[162] Y. Zhang, V. V. G. Krishnan, J. Pi, K. Kaur, A. Srivastava, A. Hahn, and S. Suresh, "Cyber physical security analytics for transactive energy systems," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 931–941, Mar. 2020.

[163] C. Chen, K. Zhang, K. Yuan, L. Zhu, and M. Qian, "Novel detection scheme design considering cyber attacks on load frequency control," *IEEE Trans. Ind. Informat.*, vol. 14, no. 5, pp. 1932–1941, May 2018.

[164] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 1–33, May 2011.

[165] B. M. Horowitz and K. M. Pierce, "The integration of diversely redundant designs, dynamic system models, and state estimation technology to the cyber security of physical systems," *Syst. Eng.*, vol. 16, no. 4, pp. 401–412, Dec. 2013.

[166] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on DC state estimation," in *Proc. 1st Workshop Secure Control Syst.*, Stockholm, Sweden, 2010.

[167] Z. Wang, Y. Chen, F. Liu, Y. Xia, and X. Zhang, "Power system security under false data injection attacks with exploitation and exploration based on reinforcement learning," *IEEE Access*, vol. 6, pp. 48785–48796, 2018.

[168] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," *IEEE Trans. Power Syst.*, vol. 31, no. 5, pp. 3864–3872, Sep. 2016.

[169] Md. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2012, pp. 3153–3158.

[170] M. Higgins, F. Teng, and T. Parisini, "Stealthy MTD against unsupervised learning-based blind FDI attacks in power systems," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1275–1287, 2021.

[171] R. Deng and H. Liang, "False data injection attacks with limited susceptance information and new countermeasures in smart grid," *IEEE Trans. Ind. Informat.*, vol. 15, no. 3, pp. 1619–1628, Mar. 2019.

[172] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1665–1676, Jul. 2014.

[173] L. Che, X. Liu, Z. Li, and Y. Wen, "False data injection attacks induced sequential outages in power systems," *IEEE Trans. Power Syst.*, vol. 34, no. 2, pp. 1513–1523, Mar. 2019.

[174] L. Che, X. Liu, and Z. Li, "Fast screening of high-risk lines under false data injection attacks," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 4003–4014, Jul. 2019.

[175] Y. Xiang, Z. Ding, Y. Zhang, and L. Wang, "Power system reliability evaluation considering load redistribution attacks," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 889–901, Mar. 2017.

[176] J. Fu, L. Wang, B. Hu, K. Xie, H. Chao, and P. Zhou, "A sequential coordinated attack model for cyber-physical system considering cascading failure and load redistribution," in *Proc. 2nd IEEE Conf. Energy Internet Energy Syst. Integr.*, Oct. 2018, pp. 1–6.

[177] X. Liu and Z. Li, "Local topology attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 2617–2626, Nov. 2017.

[178] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren, "A survey and analysis of the GNSS spoofing threat and countermeasures," *ACM Comput. Surv.*, vol. 48, no. 4, pp. 1–31, May 2016.

[179] P. Risbud, N. Gatsis, and A. Taha, "Vulnerability analysis of smart grids to GPS spoofing," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3535–3548, Jul. 2019.

[180] R. Deng, P. Zhuang, and H. Liang, "CCPA: Coordinated cyber-physical attacks and countermeasures in smart grid," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2420–2430, Sep. 2017.

[181] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Bilevel model for analyzing coordinated cyber-physical attacks on power systems," *IEEE Trans. Smart Grid*, vol. 7, no. 5, pp. 2260–2272, Sep. 2016.

[182] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Analyzing locally coordinated cyber-physical attacks for undetectable line outages," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 35–47, Jan. 2018.

[183] H.-M. Chung, W.-T. Li, C. Yuen, W.-H. Chung, Y. Zhang, and C.-K. Wen, "Local cyber-physical attack for masking line outage and topology attack in smart grid," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 4577–4588, Jul. 2019.

SAAD HAMMOOD MOHAMMED received the B.Sc. degree in computer engineering from the University of Technology, Iraq, in 2005, and the M.Sc. degree in computer engineering from the University of Turkish Aeronautical Association, Turkey, in 2017. He is currently pursuing the Ph.D. degree in computer engineering with esteemed Universiti Kebangsaan Malaysia (UKM), Malaysia. He is also a Distinguished Scholar renowned in the field of computer engineering. His Ph.D. research delves into the captivating domains of self-organization, cooperative communication, and a wide spectrum of technical proficiencies, including C++, Java, turbine control systems, thermal power plants, grid distribution (line protection), power transmission control of power electrical, generator protection on the secondary side, and gas power plants. His work exhibits a prominent emphasis on harnessing artificial intelligence (AI) and machine learning methodologies. He boasts an extensive reservoir of research experience and maintains a profound fascination for a diverse range of subjects, thereby establishing himself as a versatile and dynamic figure in the realm of computer engineering. His unwavering dedication to pushing the frontiers of knowledge within emerging technologies underscores his steadfast commitment to making substantial contributions to the academic and scientific community.

ABDULMAJEED AL-JUMAILY (Senior Member, IEEE) received the B.Sc. degree in electronics and communication engineering, the M.Sc. degree in wireless communications engineering, and the Ph.D. degrees in wireless communication and networks engineering from University Putra Malaysia (UPM), in 2003, 2014, 2018, and 2022, respectively. He is currently a dedicated professional in the field of wireless communications with expertise in mobile and satellite communications. Following his Ph.D. Research Fellow on an Erasmus + KA107 Exchange as a Ph.D. Researcher with the University Charles III of Madrid (UC3M), Spain, he started working in his current role, he did his postdoctoral research with the Signal Theory and Communications Department (DTSC), Universidad Carlos III de Madrid (UC3M). His research interests include mobile communications systems, satellite communications, radio propagation, link budget, WiFi, bluetooth, signal processing, image processing, augmented reality, digital communication, AI, machine learning, phased arrays for next-generation communication and sensing systems, analyzed measurement results, proposed mitigation techniques for 5G and fixed satellite service (FSS) co-existence at C-band and Mm-Wave based on machine learning, array optimization, cooling, multibeam antennas, front-end architectures, and beamforming algorithms. He responsible for supervising research projects, including Ph.D., master's theses, and undergraduate projects; and developing successful educational programmes and courses that inspire and challenge students. He regularly publish research articles in peer-reviewed journals to share his findings with the scientific community. Since 2017, he has been a member of the International Association of Engineers (IAENG). He is also a member of Malaysia's Board of Technologists (MBOT) and the U.K.'s BCS, the Chartered Institute for IT.

MANDEEP S. JIT SINGH received the B.Eng. degree (Hons.) in electrical and electronic engineering from the University of Northumbria, U.K., in 1998, and the Ph.D. degree in electrical and electronic engineering from Universiti Sains Malaysia, in 2006. From June 2006 to June 2009, he was a Lecturer with Universiti Sains Malaysia. He is currently a Professor with Universiti Kebangsaan Malaysia. He has published 190 articles in ISI journals. He has reviewed more than 200 articles in impact factors journals.

VÍCTOR P. GIL JIMÉNEZ (Senior Member, IEEE) received the B.S. degree (Hons.) in telecommunication from the University of Alcalá, in 1998, and the M.S. degree (Hons.) in telecommunication and the Ph.D. degree (Hons.) from the University Carlos III of Madrid, in 2001 and 2005, respectively. He was with the Spanish Antarctica Base, in 1999, as a Communications Staff. He visited the University of Leeds, U.K., in 2003, Chalmers Technical University, Sweden, in 2004, and Instituto de Telecommunicaçoes, Portugal, from 2008 to 2010. He is currently with the Department of Signal Theory and Communications, University Carlos III of Madrid, as an Associate Professor. He has also led several private and national Spanish projects and has participated in several European and international projects. He holds one patent. He has published over 50 journal articles/conference papers and seven book chapters. His research interests include advanced multicarrier systems for wireless radio, satellite, and visible light communications. He held the IEEE Spanish Communications and Signal Processing Joint Chapter Chair, from 2015 to 2021. He received the master's and Ph.D. thesis Award from the Professional Association of Telecommunication Engineers of Spain, in 1998 and 2006, respectively.

AQEEL S. JABER was born in Iraq, in 1977. He received the B.E. and M.E. degrees from the University of Technology, Bagdad, Iraq, in 2001 and 2007, respectively, and the Ph.D. degree from University Malaysia Pahang, Pahang, Malaysia, in 2015. He has been with the Department of Electrical Power Engineering Techniques, Al-Mamoun University College, Baghdad, since 2009. Until October 2021, he was an Associate Professor with the Al-Mamoun University College. Since that, he has been as an Independent Researcher in Helsinki, Finland.

YASEEIN SOUBHI HUSSEIN received the B.Sc. degree in electrical engineering from the University of Baghdad, Iraq, in 1999, the master's degree in telecommunications engineering from the University of Malaya, Malaysia, in 2010, and the Ph.D. degree in communication and networks engineering from Universiti Putra Malaysia, in 2014. He was a Consultant for the Project of Visible Light Communication (VLC) with Telekom Malaysia BHD (Berhad), from January 2015 to August 2015. He became a Postdoctoral Researcher and a Postdoctoral Research Fellow with the Faculty of Engineering, Multimedia University, Cyberjaya, Malaysia, in 2016 and 2017, respectively. He became a Senior Lecturer with the School of Technology, Asia Pacific University of Technology & Innovation, Kuala Lumpur, Malaysia, from 2017 to 2019. Currently, he is an Assistant Professor with the Department of Information Systems and Computer Science, Ahmed bin Mohammed Military College (ABMMC), Doha, Qatar. His main research interests include 5G networks, computer networks, LTE and LTE-advance, wireless channel modeling, millimeter wave technology (mmW), visible light communication (VLC), also known as Li-Fi, wireless sensor networks, heterogeneous networks, green radio resource management, cognitive radio, adaptive techniques, and cross-layer approach.

MUDHAR MUSTAFA ABDUL KADER AL-NAJJAR received the B.Sc. degree in information technology from the Majan College, University of Bedfordshire, U.K., in 2009, and the M.Sc. degree in computer science from the Mazoon College, Banasthali University, India, in 2011. He is currently pursuing the Ph.D. degree in information technology with prestigious University Tun Hussein Onn Malaysia (UTHM), Malaysia. He is also an Accomplished Scholar in the field of information technology. His Ph.D. research is centered around the fascinating realms of self-organization, cooperative communication, vision for computers, and image processing, with a strong emphasis on artificial intelligence (AI) and machine learning techniques. He possesses a wealth of research experience and a deep-rooted interest in various other areas, making him a versatile and dynamic scholar in the field of information technology. His dedication to pushing the boundaries of knowledge in emerging technologies highlights his commitment to contributing meaningfully to the academic and scientific community.

DHIYA AL-JUMEILY (Senior Member, IEEE) is currently a Professor in artificial intelligence with Liverpool John Moores University and the President of the eSystems Engineering Society. He is also a successful Entrepreneur. He is also the Head of Enterprise with the Faculty of Engineering and Technology. He has been awarded various commercial and research grants, nationally, and internationally, over £5M from Overseas Research and Educational Partners, U.K., through British Council, and directly from industry with a portfolio of various Knowledge Transfer Programs between academia and industry. He is also a Chartered IT Professional. He has published over 300 peer-reviewed scientific international publications, ten books, and seven book chapters, in multidisciplinary research areas, including machine learning, neural networks, signal prediction, telecommunication fraud detection, AI-based clinical decision-making, medical knowledge engineering, human–machine interaction, intelligent medical information systems, sensors and robotics, wearable and intelligent devices, and instruments. He has successfully supervised over 20 Ph.D. students studies and has been an external examiner to various U.K. and overseas universities for undergraduate, postgraduate, and research degrees. His current research interest includes decision support systems for self-management of health and medicine. He has extensive research interests include the wide variety of interdisciplinary perspectives concerning the theory and practice of applied artificial intelligence in medicine, human biology, intelligent community, and health care. He is also a fellow of the U.K. Higher Education Academy. He has been the Founder and General Series Chair of the IEEE International Conference on Developments in eSystems Engineering DeSE, since 2007. He has a large number of international contacts and leads or participates in several international committees in his research fields. He has one patent and coordinated over ten projects at national and international level.