Received February 10, 2022, accepted March 20, 2022, date of publication March 30, 2022, date of current version April 7, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3163551

A Comprehensive Review of Cybersecurity in Inverter-Based Smart Power System Amid the Boom of Renewable Energy

NGUYEN DUC TUYEN[1,4], NGUYEN SY QUAN[2], VO BA LINH[2], VU VAN TUYEN[3], (Member, IEEE), AND GORO FUJITA[4], (Member, IEEE)

[1]Department of Electrical Engineering, School of Electrical and Electronic Engineering, Hanoi University of Science and Technology, Hanoi 100000, Vietnam
[2]Department of Industrial Automation, School of Electrical and Electronic Engineering, Hanoi University of Science and Technology, Hanoi 100000, Vietnam
[3]Electrical and Computer Engineering Department, Clarkson University, Potsdam, NY 13699, USA
[4]Department of Electrical Engineering and Electronics, Shibaura Institute of Technology, Tokyo 135-8548, Japan

Corresponding author: Nguyen Duc Tuyen (tuyen.nguyenduc@hust.edu.vn)

ABSTRACT The blossom of renewable energy worldwide and its uncertain nature have driven the need for a more intelligent power system with the deep integration of smart power electronics. The smart inverter is one of the most critical components for the optimal operation of Smart Grid. However, due to the deep information and communication technology (ICT) infrastructure implementation that most inverter-based smart power systems tend to have, they are vulnerable to severe external threats such as cyberattacks by hackers. This paper presents a comprehensive review of the system structure and vulnerabilities of typical inverter-based power system with distributed energy resources (DERs) integration, nature of several types of cyberattacks, state-of-the-art defense strategies including several detection and mitigation techniques, and an overview and comparison of testbed and simulation tools applicable for cyber-physical research. Finally, challenges, unsolved problems, and future direction of the field are discussed and concluded at the end of the journal. This paper provides an all-inclusive survey at the state of the art smart grid cybersecurity research and paves the path for potential research topics in the future.

INDEX TERMS Cybersecurity, cyber-physical system, smart grid, false data injection, self-security, DER, renewable energy.

ABBREVIATION

AMI	Advanced Metering Infrastructure.
API	Application Programming Interface.
CPPS	Cyber-Physical Power System.
CPS	Cyber-Physical System.
CPSG	Cyber-Physical Smart Grid.
DER	Distributed Energy Resource.
DoS	Denial-of-Service.
EMS	Energy Management System.
HMI	Human-Machine Interface.
ICT	Information and Communication Technology.
IT	Information Technology.
LAN	Local-Area Network.
PV	Photovoltaic.
RE	Renewable Energy.
SCADA	Supervisory Control And Data Acquisition.
VSI	Voltage Source Inverter.
WAN	Wide-Area Network.

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

I. INTRODUCTION

A. BACKGROUND AND MOTIVATION

It is common knowledge that renewable energy development is inevitable due to the rise in concern of climate change and demand for a cleaner energy supply source. Thanks to several clean energy transition movements, the mass implementation of solar and wind energy has been thriving in recent years. The realization of a carbon-neutral electrical network is among the most important global technology goals. This would not only cut pollution and global warming but would also diminish society's total reliance on a volatile supply of fossil fuels. The German government has stated that it will adhere to the objective of reducing greenhouse gas emissions by 40% by 2020 and by 80-95% by 2050, and renewable energy sources must account for at least 35% of total power generation by 2020, and 80% by 2050 as stated in [1]. As promising as it sounds, renewable energy development also leads to several technical and economic problems that should be considered. Such problems could be voltage and frequency instability, overloading of transmission lines, demand/supply unbalance, and so on. In order to solve those issues, the implementation of an intelligent power grid with the integration of ICT is necessary. Such an integrated system is often referred to as a CPSG, a part of the CPS trend that has been popular recently in various industries due to the rising demand for more efficient operation and ''smarter'' working environment across all sectors. However, since the computation system of the CPS, including the CPSG, often has to perform various advanced tasks in sensitive environments, the data collecting, data processing, and system control functions are becoming more and more complicated than before. It can potentially lead to vulnerabilities never before seen in conventional industrial systems. A typical monitoring and control structure of a smart ''microgrid'', a self-sufficient energy system with a specific geographic footprint, can be seen in Fig. 1 [2].

B. CURRENT SECURITY ISSUES OF SMART GRID

CPSG often collects data regarding the current, voltage measurements, or grid status through the system of sensors and meters to perform particular actions such as control action or protection procedure against system malfunction or fault condition. From a centralized point of view, it might be dangerous if attackers can manipulate those data, resulting in massive system malfunction on many different levels. Since the cyber-physical grid often has to work in real-time in a sensitive environment, the threat of cyber and physical instabilities on the grid's performance can be extremely severe and difficult to react to without proper control methods and error mitigation strategies. However, the incorrectness of data obtained from measurement components is not the sole cause of system instability. The modern smart grid often utilizes power electronic devices such as transistors, converters, inverters with digital features, which could also be the root of CPS uncertainties. Power electronic data could be voltage and current measurements, error flags, along with pulse width modulation references. FDIA, unintended failures, and cyber-physical switching attacks are only a few of the significant risks, attacks, and defects that can befall power converter components [3]. Furthermore, due to the integration of power electronics, attackers can also take advantage of their accompanying systems such as battery energy storage system (BESS), grid-connected charging station, RE farm network, as an intermediate environment to conduct cyberattacks on the control entity of the CPS. To ensure the reliability of the system, appropriate fault detection strategies, as well as precise signaling of faults, are essential.

There are several approaches to cybersecurity in CPSG with power electronics integration. CPS attack countermeasure must be accomplished through security strategies that employ detection and mitigation methodologies to protect various system levels. Such techniques can be classified into prevention, detection, or response approach [4]. The prevention approach refers to the encryption mechanism as well as highly secured network protocols. The point of this approach is to stop the intrusion from happening anywhere in CPS. Smart inverters, for example, have a self-healing feature that can filter out malicious signals and quickly recover their desired state. More information regarding the self-security feature of the smart inverter will be discussed in a later section. However, the prevention approach is often expensive and somewhat impractical because it requires a synchronous development of all components within a system, including all the standards and protocol, to be truly effective, which is not ideal for most cases due to budget limitations. On the other hand, system-level attack detection techniques are designed to recognize the irregular behavior of the system when a cyberattack occurs. These techniques are often categorized into model-based methods and data-driven methods. Model-based detection method detects anomaly based on the characteristics of system's model extracted from state estimation algorithm. From that foundation, a detection index will be created to identify anomalies that go against the desired operation; then, a self-healing control strategy will be proposed to restore the system to regular operation. Authors in [5] illustrate the basics of model-based defense strategy for grid-tied power converter in a typical DC or AC Microgrid. Being able to model the system characteristics is critical for this method. The model-based approach is often considered reliable and has high efficiency; however, it requires an accurate model of the whole system, which is not ideal for implementation on an extensive system like the national transmission grid. On the other hand, the data-driven method utilizes data mining and machine learning methods to detect intrusion based on the training set of past data and data collected from instruments in real-time. Several methodologies regarding this method can be seen in [2]. Authors in [2] also mention the cyber-based method that targets the protection of ICT infrastructure. Cyber-based methods detect anomalies by utilizing IT data retrieved from electronic components and communication networks, and they are generally divided into network-based, and host-based approaches [6]. While network-based approaches collect and analyze communication packets as well as network behavior, host-based methods detect intrusion footprints in host devices by analyzing activity logs, and system file integrity [7]. Even though the cyber-based attack is a trending topic, our research focuses mainly on the physical and cyber-physical-based attacks.

C. LITERATURE REVIEW ON PREVIOUS SURVEYS

In recent years, various survey papers related to the cybersecurity problem in CPS and power systems have been written. In 2017, authors of [8] conducted an overview of potential research topics in the field of smart grids. They also demonstrated the existing simulation testbed's

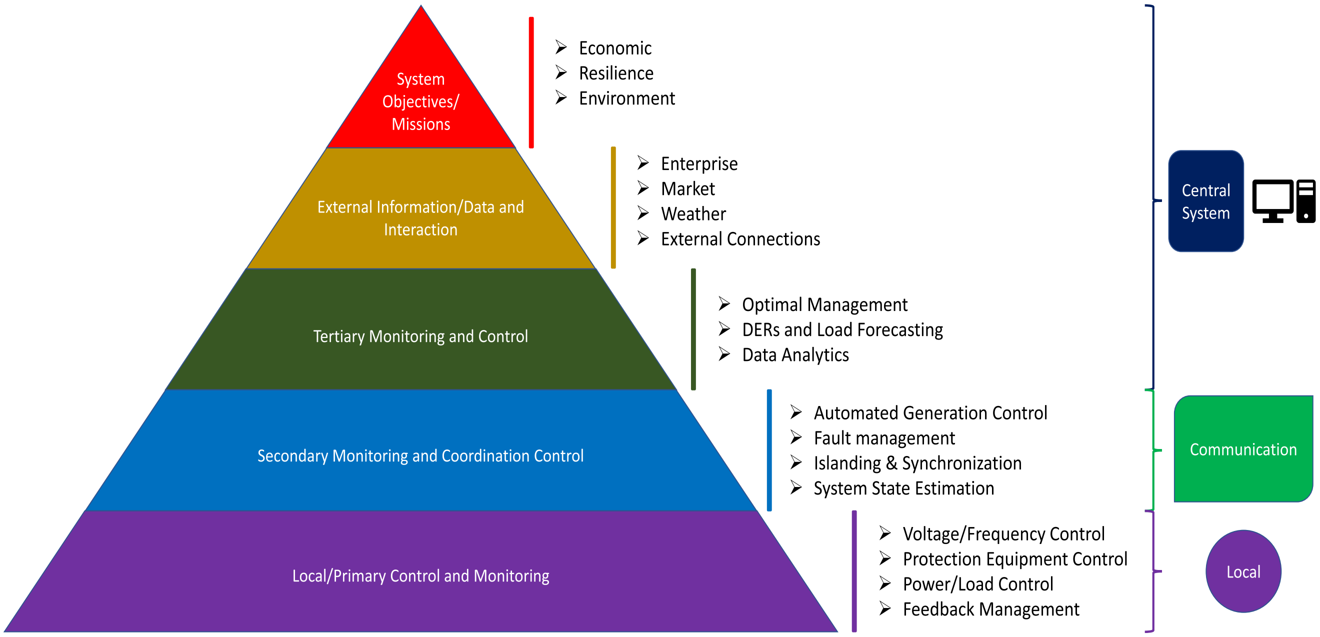
System Objectives/ Missions
Economic
Resilience
Environment
External Information/Data and Interaction
Enterprise
Market
Weather
External Connections
Tertiary Monitoring and Control
Optimal Management
DERs and Load Forecasting
Data Analytics
Secondary Monitoring and Coordination Control
Automated Generation Control
Fault management
Islanding & Synchronization
System State Estimation
Local/Primary Control and Monitoring
Voltage/Frequency Control
Protection Equipment Control
Power/Load Control
Feedback Management
Central System
Communication
Local

FIGURE 1. **Overview of the monitoring and control functions of a typical microgrid, including possible layers for cyberattack.**

survey to provide a taxonomy and insightful guidelines for developing and identifying the significant features and design decisions while emerging future smart grid testbeds. However, no in-depth analysis and recommendation for usage regarding simulation tools and testbeds are made in that survey. In [9], intelligent sensing techniques and data-driven monitoring and fault diagnosis are presented to detect cyberattacks on the CPPS effectively. Theories regarding state estimation and data-driven controller design are demonstrated in that study. Reference [10] illustrates the mechanism of the infamous FDIA, which is widely popular in the field of the power system. The concept of model-based defense method and data-driven defense is also mentioned and clarified in their work. Moreover, microgrid structure and control system are depicted in [11]; authors of such study also give an overview of simulation testbed used specifically for microgrid cybersecurity research. In 2020, authors of [12] conducted a highly influential survey to review the modeling, simulation, and cybersecurity analysis in CPPS. Their work focuses mainly on the mathematical modeling aspect of the CPS. Even though the list of simulation tools, experimental software, taxonomies, attack types, and defense strategies featured in that study is relatively comprehensive, it still lacks the in-depth technical comparison and related recommendation, making it not an ideal survey material for those new to the field. In [13] published in early 2021, authors focus mainly on the mitigation approaches of power electronic systems with security challenges for smart grid applications. They present a comprehensive background of CPS security and demonstrate potential threat sources, vulnerabilities, and impact of malicious attacks on the power-electronic-based power grid. Even so, since the main focus of such study is the theoretical background and foundation of vulnerabilities and operating principle of CPS and smart grid, the in-depth analysis and comparison of defense strategy, the classification of detection and mitigation strategy based on their characteristics and field of application as well as the detailed overview of simulation tool and experimental procedure are all still absent. Moreover, such study does not feature defense strategies for other types of cyberattacks such as DoS and does not review the prevention approach, which is equally important in the cybersecurity industry. Later in 2021, authors of [14] conducted a review of challenges and opportunities for cybersecurity in power grids. The study elaborated security issues of power system communication, security issues of power generation and successfully demonstrated various attacks scenarios as well as prevention, detection, and mitigation methods for FDIA and DoS. However, the review of the prevention and detection method of such study is still too general and does not take a deep dive into the specific applicable methodologies and technologies for each possible vulnerability.

Overall, all surveys and review journals up to this point usually focus too much on describing smart grid technology and only tackle a small portion of security challenges; an in-depth, comprehensive survey that covers all aspects of smart grid vulnerabilities, possible defense mechanisms, and recommendation on simulation tools and testbed selection for security research has not been made.

D. OUR CONTRIBUTION

Learning from the state of all related publications as well as the aforementioned trend of development in the energy industry, the goal for our study is to conduct a

TABLE 1. The comparative study of the scope of our journal.

Journal ***Year of Publication***	**[8]** ***2017***	**[9]** ***2018***	**[10]** ***2019***	**[11]** ***2019***	**[12]** ***2020***	**[13]** ***2021***	**[14]** ***2021***	**Our work**
Overview of SG technology	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Vulnerability analysis of Inverter & Controller	🟥	🟥	🟩	🟥	🟥	🟩	🟩	🟩
Vulnerability analysis of IoT-based devices & AMI	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟩
Vulnerability analysis of EMS and HEMS	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩
Survey of Detection mechanism for FDIA	🟥	🟥	🟩	🟥	🟩	🟩	🟩	🟩
Survey of Detection mechanism for DoS	🟥	🟥	🟥	🟥	🟩	🟥	🟩	🟩
Survey of Prevention mechanism	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩
Self-secured Inverter Review	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩
Review of Simulation tools and Tesbed	🟩	🟥	🟥	🟩	🟩	🟥	🟥	🟩
Comparative study of simulation tools & testbed	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟩
Recommendation on Testbed selection	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩

🟥 Not featured in the study 🟩 Featured in the study

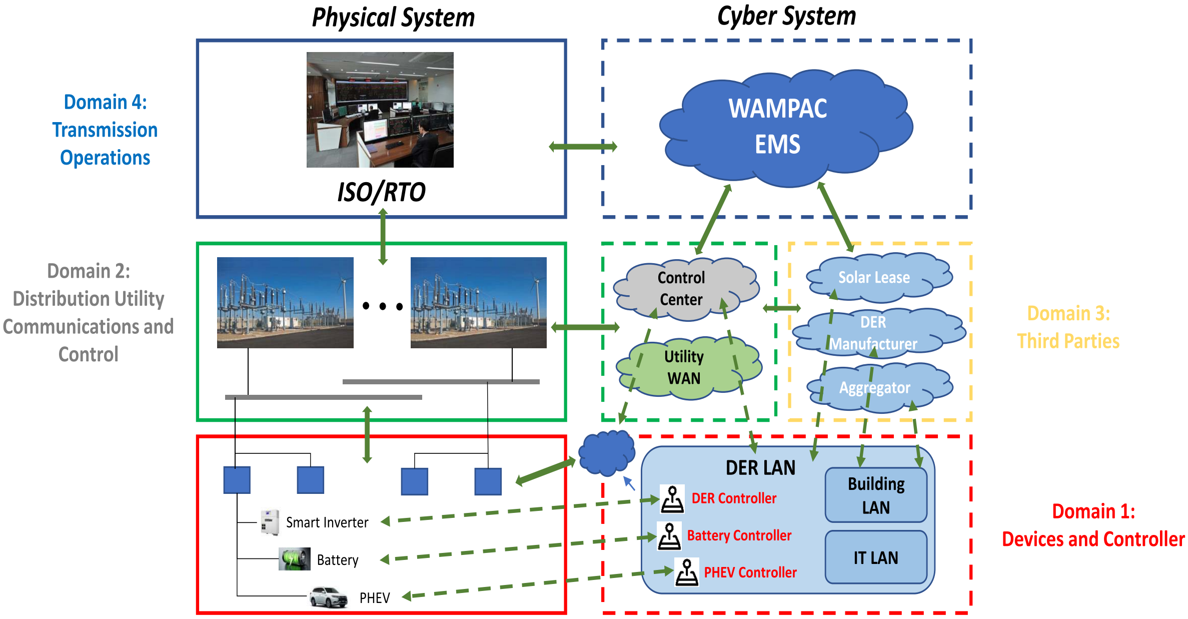

FIGURE 2. The 4-domain architecture of DER system.

comprehensive and complete review journal to effectively analyze the technology used for CPPS with integration of power electronics and renewable energy systems amid the rise of cybersecurity issues. The specific scope of our work is cybersecurity on the physical and cyber-physical aspects of an inverter-based smart power system with the integration of renewable energy systems, charging stations, DER, and BESS. The main contributions of our study are:

- Comprehensively illustrate an overview of the vulnerabilities of grid supportive services and DER technologies in CPPS, demonstrate the unpredictability of cyberattacks that can be conducted to attack smart grid from various sources.
- Summarize the state-of-the-art detection and mitigation methods for cyberattacks in inverter-based power system updated up to the recent period.
- Illustrate the self-security and self healing philosophy of modern smart inverter in power system and its principle, which can be a great alternative to other system-level defense mechanism.
- Survey the up-to-date simulation tools and testbeds that could be used to research in this field. An extensive comparative study is also proposed to give recommendations for appropriate usage.
- Existing challenges, potential solutions, and a new future direction for the topic including discussion of artificial intelligence, resilience philosophy and blockchain are concluded in the final sections of this journal.

The graphical comparison between our study and other similar reviews can be seen in Table 1, in which our contribution regarding state-of-the-art defense strategy survey against FDIA and DoS, review of prevention mechanism and self-secured inverter technology, comparative study, and recommendation of simulation tools and testbed are highlighted.

E. PAPER STRUCTURE

This paper is organized as follows: Section II presents Assessment of vulnerabilities and threats of CPSG. Section III illustrates the state-of-the-art defense strategy against cyberattacks on smart grid, including both preventative methods and detection and mitigation methods. Section IV presents the overview of simulation tools and testbed as well as its comparative study and recommendation. Section V offers current challenges, potential solutions, and future direction. Conclusion regarding the research topic is made in the final section.

II. VULNERABILITIES OF INVERTER-BASED POWER SYSTEM

In the inverter-based smart grid, various components can be exploited by cybercriminals such as DER systems, communication and telecommunication devices, WAMPAC application, IoT devices, EMS, solar, and wind energy facilities, and also inverter and power electronic devices. This section demonstrates a precise overview of the possible cyber weaknesses of an inverter-based smart power system from all aspects of the system, reviewing the potential vulnerabilities from the very top-level DER system to individual power electronic devices and local controllers.

A. GENERAL VULNERABILITIES OF DER SYSTEMS

An attack against DER systems could be conducted on multiple devices and communication networks owned by either utilities or DER private owners. The severity of attacks on the various system components and entities depends on the size of DER and its quantity. Regarding DER system architecture, authors in [15] proposed a 4-domain structure that comes in handy for cybersecurity research. The first domain is DER devices and controllers in which DER is owned and controlled by consumers who get economic advantages by generating power for personal use and selling excess power to the utility. This domain includes DER, grid-connected energy storage system, electric vehicles (EVs) with two-way power exchange capability, smart inverter, and LAN network. The second domain is called Distribution Utility, Communication, and Control. As an actor in this field, the utility company can send control commands to smart inverters, such as DER connect/disconnect, adjust voltage, and manage the allowable penetration level. In this domain, utilities often utilize Smart Power Profile (SEP) 2.0 to interact with smart inverters and controllers. The third domain is about integration with third-party systems, including Solar Lease, DER manufacturer, and aggregator. The final domain is related to transmission operations, including centralized generation units and independent system operators (ISO) and regional system operators (RSO). The cyber system of the DER network is usually Wide Area Monitoring Protection and Control (WAMPAC) EMS, handling state estimation, automatic generation control, security-constrained optimal power flow (SCOPF), and remedial action scheme (RAS). The summary visualization of such architecture can be seen in Fig.2. It is important to note that each domain features its vulnerability points, ranging from unauthorized access, attack through communication networks to the utilization of third-party devices and measurement data manipulation. The detailed list of vulnerable points in all four domains is presented in Table 2 below. The following part of this subsection will be about threat scenario analysis of such vulnerable points.

B. ATTACK ON INVERTER AND DER CONTROLLER

In general, a diverse set of digital devices is frequently required to handle the operation of the DER system and provide both consumers and utilities with adequate information regarding their operation. Smart inverters, as well as DER controllers, will almost certainly be included in nearly every DER system; others might also involve battery controllers and sometimes controllers for EVs. If access to these systems is available, adversaries can take over their control functions and spoof status information to utilities or DER owners. Attack methods that can directly manipulate smart inverters can be particularly problematic because they may intelligently deceive the device's function based on the state of the power system, leading to undesirable grid states.

Taking inverter further into consideration, inverters in the power system can be classified into voltage source inverter (VSI) and current source inverter (CSI). VSI, in particular, can be categorized further into the grid-forming inverter, grid feeding inverter, and grid supporting inverter. The function of grid forming inverter is to regulate voltage and frequency locally. In general, the synchronization of the inverter with other AC sources is often deployed by the utilization of a primary droop control system, which is often considered well-secured against external intrusion on the physical layer. In addition, suitable physical layer security alternatives, such as beamforming, are also commonly used to increase the resiliency of the primary control system [16]. However, such decentralized control systems often have trouble complying with commercial, regulatory standards [17] and are usually required to utilize a secondary controller that uses data collected from other VSIs [18]. Whether centralized or distributed, secondary control strategies can be imposed on the primary control law for offset compensation function. However, such utilization can result in a sizeable vulnerable space for cybercriminals to find the attacked data, whether in the controller, the communication link, or the sensors.

Furthermore, adversaries can gain access to the control platform through a sensors system by utilizing Trojan Horse [19] method. It is essential to know that the output voltage from the acquisition panel is usually within 15 V, and acquisition gains can be used in conjunction with a linear plotting system to modulate it alongside the actual measurement. Commonly, the acquisition gains are often altered by attackers to create a bias in the reported measurement, and therefore, attackers successfully conduct an intrusion into the system through sensors. Another way to attack is through communication links; attackers can manipulate the communicated data both inside the controller and in the communication stage, including routers, encoder, decoder. There are several ways to manipulate the data, such as authorization violation, interruption of transmission

TABLE 2. Cyberattacks vulnerability of 4 domains in DER system.

No	Domain	Interaction	Vulnerabilities
1	DER devices & controller	DER owners can obtain DER information by communicating with DER through wireless technology or human-machine interface (HMI). Facilities DER energy manegement system (FDEMS) can interact with DER through LAN/WAN network.	+ Unauthorized access to DER controllers and smart inverter + Penetration through facility network + Malicious attack on smart meters + Alteration of settings in FDEMS + Owners who are inexperienced and fail to properly secure their devices
2	Distribution utility communication & control	Communication protocols such as smart energy profile (SEP) 2.0 are used by the utility to interact with the smart inverters and controllers in a DER-connected power system.	An intruder could gain access to the utility network. Malicious commands sent to DER controllers and/or meters can lead to problems.
3	Third-parties	The majority of third-party entities can track the condition of DER, and some may even be able to directly manipulate their operation. These entities can in fact get access to a large quantity of DERs. For maintenance purposes, DER devices are often configured to communicate directly with the manufacturers or utility companies, which means those companies can remotely control a large number of DERs within a power system.	These interconnections create centralized points that attackers might potentially utilize to modify DER instances. Third-party systems may directly interconnect with many more DER instances, influencing a large number of DER across multiple distribution grids.
4	Transmission Operation	Even though ISO/RTO does not directly control the DER system, it can still determine what DER systems are required to do. The operation of the power grid at the ISO/RTO level can also have an influence on DER activity. DNP3 and IEC 61850 are two commonly used communication protocols in this context.	Attackers can compromise important measurement value and disrupt several advanced applications in this domain such as EMS, inflicting severe voltage and frequency violation.

of signals, the illegitimate opening of information logs, replaying the transmitted information from the past. Last but not least is the intrusion method through the controller system. As previously stated, the controller can be illegally accessed using Trojan Horse to change the reference inputs employed in the outer control loop or secondary controller for VSI control.

Grid-feeding control for VSIs is often employed in various grid-tied applications to inject active and reactive power into the previously mentioned grid-forming unit [20]. With the aim to intensify the performance of grid-supporting services, the targeted control inputs are included in the overlaying grid-forming controller. There are usually two ways that adversaries can utilize to attack services provided by grid-feeding and grid-supporting inverter. Firstly, hackers can disrupt the stability and coordination of the power grid by interfering with the power flow from the VSI to alter the value of command voltage and measured voltage. Another way is to mislead the controlled units in the power-electronic-based power system by injecting false data into the grid supportive service; this second attack strategy is false data injection attack (FDIA).

As mentioned earlier, the VSI local control system can support network frequency control. In fact, under moderate frequency deviation and rate of change of frequency (ROCOF), modern grid codes mandate converters to remain connected and proceed to exchange power with the grid. [21]. Because of the frequency response from VSIs, adversaries can alter the active power set-point tying in with grid frequency fluctuation (from 50Hz to 49.5Hz at $t = 0.12$ s) by either attacking the system frequency through a distributed controller or attacking the system voltage with the FDIA. These FDIAs are executed on the controller by an intrusion method, adding a bias to the measured voltage detected by the data acquisition unit or to the frequency value obtained by the phase-locked loop (PLL), so the control theory is manipulated by illegal measurement.

It is also important to note that the integration of renewable energy on a large scale due to its intermittent nature often leads to violations of voltage regulatory restrictions [22], which result in the disconnection of VSI as well as voltage stability problems [23]. Even though several local voltage control strategies for VSI are proposed in [24], [25], only when the local parameters are tuned centrally with the aid of AI-based day-ahead prediction of RE sources and load profile is the optimal operation achieved. In order to tackle this problem, authors in [26], [27] proposed a robust multi-step voltage control mechanism that provides reactive power support for the VSI system. These local reactive power supportive control mechanisms can optimize on-load tap changer (OLTC) tap changes based on the minimum and maximum voltage set points and are also capable of limiting voltage fluctuations in the narrow band. All of these advanced control strategies are expected to handle system fluctuation when FDIA is initiated in the measurement of the bus within the system and have been proven relatively resilient in most cases. However, in the worst-case scenario of injecting a large amount of spurious data into the system, it can diverge beyond the maximum voltage threshold, resulting in unnecessary OLTC operation. Furthermore, coordinated attacks that combine several methods can be tricky for these controllers, leading to the need for research of more advanced synchronization strategies and recovery mechanisms.

C. ATTACK ON COMMUNICATION SYSTEM

Controlling the operation point, managing device status, and maintaining the reliability of the distribution grid all require remote communication among utilities and DER infrastructures. However, if cyberattacks disrupt this communication,

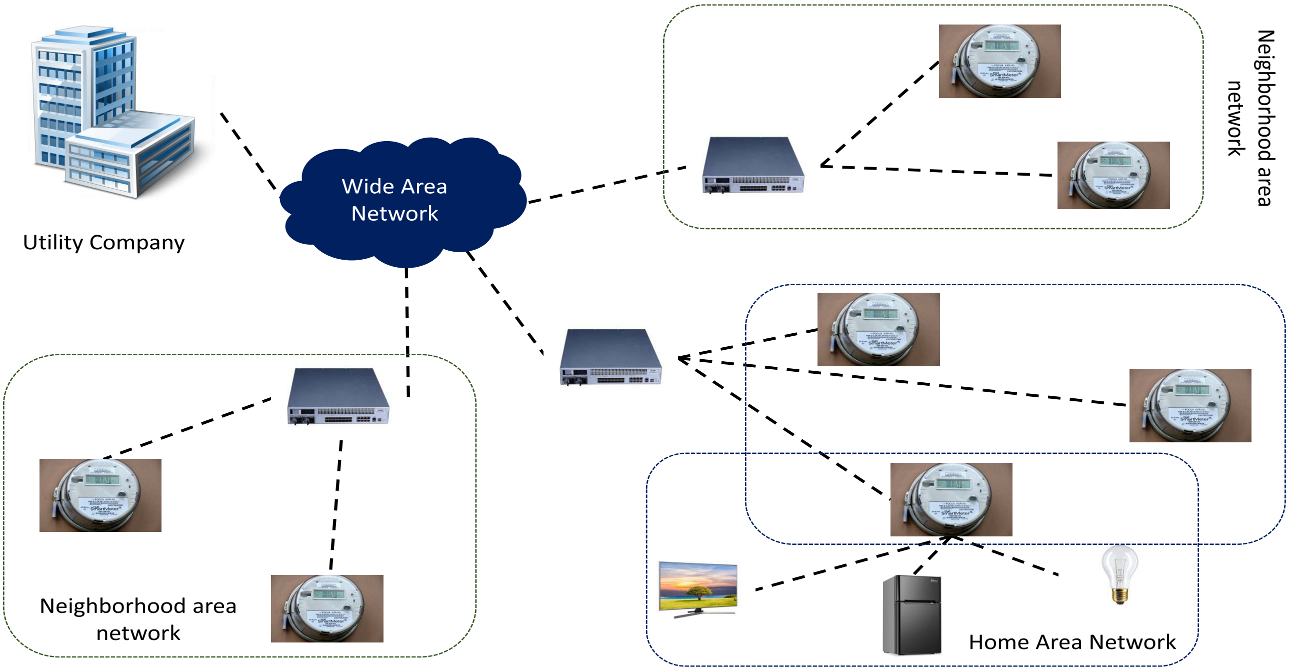

FIGURE 3. The interconnection nature of advanced metering infrastructure.

utilities will be unable to perform necessary control actions. These attacks can be caused by the presence of a variety of vulnerabilities, such as insecure network protocols, the mishandling of cryptographic operations, or unauthorized intrusion into utility DER systems. Such attacks have the potential to provide hackers with the ability to take over a great number of DER, having a significant impact on the distribution grid [28].

D. ATTACK ON WAMPAC APPLICATION

One of the most critical components of the DER system, the WAMPAC, can potentially be a target for cybercriminals since its operation is heavily tied to the efficiency of the power grid. To be more specific, attacking several critical WAMPAC applications such as automatic generation control (AGC) or remedial action scheme (RAS) could result in system-level voltage and frequency issues, significantly affecting the operation of a great number of DERs and inflicting several severe problems in distribution as well as transmission grid.

AGC is critical to modern power systems because it keeps grid frequency within acceptable bounds. Because AGC is usually the sole automatic feedback loop between the cyber layer and physical infrastructures, it is extremely susceptible to cyberattacks and thus necessitates immediate investigation [29]. Recent studies show that malicious data attacks on AGC are feasible [30]–[34]. Commonly, cyberattacks on AGC can be initiated through the falsification of sensor measurement. As illustrated in [35]–[40], the manipulation of frequency and tie-power measurements obtained from remote sensors can disrupt the operation of AGC, which can be taken advantage of by cybercriminals to initiate FDIA on the SCADA center and mislead the system dispatcher, causing massive economic and technical damages. Apart from attacks on sensors and measurement infrastructures, several studies have investigated the likelihood of attacks involving substation anomalies, which can result in cascading events [30], [32]. Furthermore, it is important to keep in mind that the protocols used in the AGC network often are DNP3, Modbus, IEC61850 as well as ICCP [35], all of which are not built with sufficient security mechanism by default. Attackers can make use of those weaknesses to disrupt the communication channel of the power system with AGC implementation. It should also be noted that conventional AGC systems employ less secure SCADA networks that are expected to function without hardware or software upgrades. As a result, high-security modern patches, firewalls, and the most recent communication channel encryption are frequently incompatible with SCADA systems, as they would necessitate endpoint compatible hardware and software.

E. ATTACK FROM IoT DEVICES CONNECTED TO INVERTER-BASED SMART GRID

The potential interconnection between DER and other systems and networks, including IoT devices as well as third-party cloud system service, can raise opportunities for cyberattacks since those infrastructures might not feature a strong security posture and can provide adversaries with remote access to the DER components. Attackers could take advantage of these connections to obtain access to the DER system and create fake commands and messages to send to the system from external sources, significantly affecting the operational settings of the DER-utilized power grid. These flaws could be the result of inadequate mechanism authentication or software flaws.

It is also important to note that resource-constrained IoT devices lack computing power, memory, and storage compared to conventional computers and mobile phones [41]. Some devices could be used remotely in various locations powered by batteries. Eventually, these devices are incapable of processing manage antivirus software and cryptographic algorithms required for critical security protocols, exposing them to greater risk. The interconnection of IoT devices may make an opening for cybercriminals to launch multiple attacks at the moment they have gained access to a network. Various attack strategies can be listed as gateway attacks, side-channel attacks, FDIA, Sybil attacks, routing attacks, as well as physical tampering [42]. To deal with this problem, apart from increasing the security feature of third-party systems, which is not a practical solution, it is essential to have a system-wide distributed attack detection and mitigation method that can effectively isolate compromised components from the system and maintain the system stability. Moreover, it is essential to strengthen the security protocol, develop robust government policies and industry standards among vendors to ensure the quality of IoT devices' security features.

Among IoT-based systems connected to the inverter-based smart grid, electric vehicle is one of the most essential elements that should be taken into consideration. For charging and discharging their batteries from/to the grid, electric vehicles can communicate with the smart grid via distributed and/or centralized vehicle-to-grid (V2G) networks. Such communication is conducted through a collector or data aggregator, a device that acts as a collector of accessible vehicle power while charging and supplying power to the vehicles via charging stations. In order to coordinate the charging operation, aggregators often have direct connections to the authentication and communication servers of the inverter-based power system. Such broad access of aggregators could make the V2G-tied grid vulnerable to various forms of cyberattack from adversaries, such as MITM [43], DoS [44] and replay attack [44]. Regarding the DoS attack, a flood-based DoS attack can be conducted by the adversary by submitting an overwhelmingly large amount of charging or discharging requests to the aggregator, constructing half-open connections, and denying to close them, eventually exhausting the aggregator's network resources. This would result in a DoS for legitimate vehicles that require power from the grid [45]. V2G is an important feature of the smart grid, and with the rapid rise of electric vehicles across the world in recent years, its cybersecurity issues are among the most discussed topics in the energy industry.

F. ATTACK ON METERING INFRASTRUCTURE

In the smart grid, advanced metering infrastructure is, in fact, the most crucial component since it enables the grid's ability to have efficient two-way communication and become more intelligent. As the deployment of Advanced Metering Infrastructure (AMI) illustrated in Figure 3 has increased, so has the security of this technology. Utility companies, energy markets, and regulators are drawn to AMI to facilitate real-time data collection on power flow and usage. This will enable utilities to offer dynamic pricing services, demand-side management, and improved grid management, though these new capabilities will potentially ramp up the attack surface [46], [47].

Similar to the vulnerabilities mentioned above of IoT devices connected to the grid, components of AMI such as smart meters and phasor measurement units (PMU) are also IoT-based. They feature similar vulnerabilities such as lack of computing power for antivirus software and cryptographic algorithms required for security protocols, lack of proper security standard, and unprotected interconnection. AMI, like any emerging system, has yet to develop security countermeasures to deal with cyberattacks that go beyond the fundamental measures commonly used, such as network encryption. The complexity, magnitude, and influence of an attack on AMI can vary significantly. A cyberattack on AMI may include gathering intelligence, infecting target AMI systems, AMI exploitation, and even data exfiltration from various AMI attack points [48].

Apart from smart meters, sensors and sensor networks are also a trending topic in the cybersecurity field since they are popular with the discussion in DoS attack research. Originally utilized in the military sector, wireless sensor networks (WSN) are used by utility companies and suppliers for substation automation management, and they are also widely utilized in wireless automatic meter reading (WAMR) systems. Energy usage and management information, including energy usage frequency, phase angle, and voltage values, can be obtained in real-time from remote devices using the WSN [49]. However, wireless sensor networks pose cybersecurity and privacy challenges to smart grids. For example, cascading-failure-induced disasters may occur if attackers disrupt the grid at a later date from a remote location; smart grid customers' privacy information may be illegitimately accessed via the WSN, and the unauthorized party may also jeopardize selected nodes in a tactical delay-tolerant network, thereby failing to disrupt the mission of SCADA systems [50], [51]. These vulnerabilities drive the need for more research and investigation in the security of WSN. Nonetheless, common WSN challenges include probabilistic channel behavior, accidental and directed interference or jamming, and eavesdropping or unauthenticated reconfiguration of communications if authentication and encryption solutions are not used [52], which all need to be solved in future studies.

G. ATTACK ON RENEWABLE ENERGY FACILITIES

1) CYBERATTACK IN WIND-BASED SYSTEMS

Due to the mass implementation of VSIs in grid-tied applications, including wind farm and RE-based microgrid, several robust and highly efficient control systems have been proposed in [53] to obtain maximum output potential. Traditionally, wind farms utilizing squirrel-cage induction generators (SCIG) often require large capacitor banks for reactive power to be absorbed by the IGs. If there is a rise in reactive power requirement, such wind farms will withdraw from the grid, and excessive withdrawal can end up causing the deterioration of voltage profile. To tackle this problem, a static compensator (STATCOM) is often employed at the PCC to provide reactive power support [54]. However, since STATCOM devices are rarely used to maximum capacity all the time, adversaries can take advantage of such under-utilization to inject FDIA on the AC voltage sensor in the inverter-based power system, causing worth-noticing disturbances.

The strategy of attacking voltage sensors is also utilized in other advanced components of wind-based systems called Grid-side Converter (GSC) in Doubly-Fed IG (DFIG). The DFIG technology allows maximum energy extraction from wind for low speeds by optimizing the speed of wind turbines in parallel with turbine mechanical stress regulation function. In the DFIG architecture, authors in [55] used two back-to-back converters to increase the active power capacity by 40%. These two converters are called rotor-side converters, and their purpose is to maximize the power output from IG using power-tip speed ratio graph [56]. The GSC governs the DC voltage to allow the power from the RSC to be transferred to the AC grid, which can be either an AC microgrid or transmission grid. As stated above, hackers can alter the voltage sensor measurement to push up the DC voltage value. As a result, the significantly high DC voltage can affect the GSC control dynamic and invoke system tripping. Having said that, a simple attack on the outer layer control loop can cause a large renewable generating unit to shut down or trip, putting its reliability in jeopardy. During the rise of renewable energy, cybersecurity countermeasures for RE farms are undoubtedly critical and require extensive research to maintain the sustainable growth of this industry.

2) CYBERATTACK IN PHOTOVOLTAIC SYSTEM

Unlike wind-based systems, solar energy can be implemented not only in solar farms but also in residential areas incorporated with the civilian power system, making its overall structure much more complicated, therefore opening more vulnerabilities. From the cyber-physical point of view, several attack points in a typical photovoltaic-based power system can be seen in Fig. 4.

From the cyber-physical point of view, the most common type of attack in the cyber-physical PV system is the one targeting the inverter controller and control algorithm. This action can be achieved by utilizing the vulnerabilities of PV plant monitoring and diagnostics systems, internet-enabled communications, or plant controllers. Furthermore, since PV inverters often feature several advanced electronic components such as digital signal processors, microcontrollers, or smart Application-specific integrated circuits, attackers can implement malicious software in these components, resulting in the corruption of inverter operation and device failure. Another strategy for cybercriminals is to attack the monitoring and diagnostics platform directly, taking advantage of the growing digitization of PV systems, including the utilization of IoT devices to communicate, send, and gather data from the PV plant. Finally, hackers can launch cyberattacks on the grid that have the ability to disrupt plant operation dramatically and overall safety (e.g. faking energy demand, isolating the plant from the grid). As a result, this can isolate PV inverters from the grid by tripping breakers or provoking low-voltage, high-voltage, or zero-voltage circumstances. A demonstration of a cyberattack model on PV converter, as well as the in-depth review of security assessment and countermeasures, can be viewed in [57].

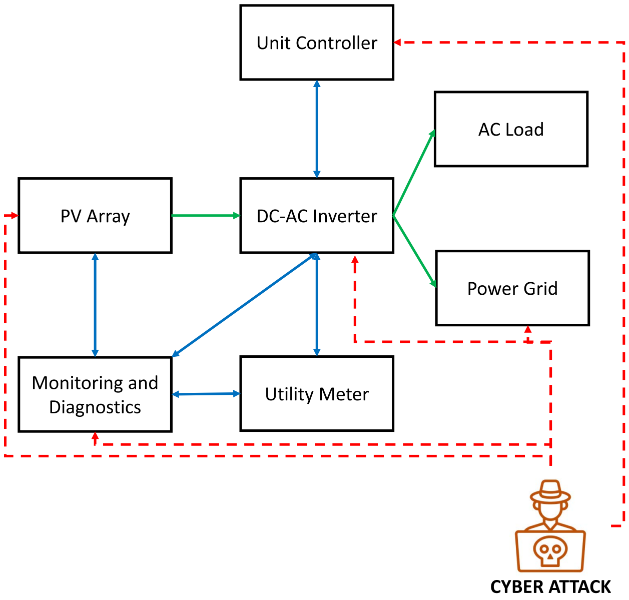

FIGURE 4. Potential photovoltaic (PV) plant cyberattack points.

H. ATTACK ON ENERGY MANAGEMENT SYSTEM (EMS)

EMS is a beneficial tool to manage power generation from different sources while obtaining its economic benefits [58], [59]. Up till now, dispatching of power generation has generally been implemented centrally to minimize operating costs using hierarchical optimization stages including integer planning [60] and artificial intelligence technology [61]. However, distributed controllers with excellent performance against cyber layer deformity have recently sparked a lot of interest, owing to the need for greater control flexibility in the face of transmission delay and information failure. [62]. From the cybersecurity point of view, attackers tend to increase the cost of power generation by intruding key parameters, with the goal of reducing the energy efficiency of the system [63] and leading to major economic loss for the grid operator. On the other hand, adversaries can also attack EMS by using stealthy deception attacks to interfere with the SCADA system in order to achieve the very same goal [64].

III. STATE-OF-THE-ART OF DEFENSE STRATEGY

A. CYBERATTACKS DISCUSSION

In general, cyberattacks on smart power system often can involve denial-of-service (DoS) [65], FDIA [66], man-in-the-middle (MITM) attack, energy theft, malware insertion, delay attack [67] and even jamming attack [68]. There are also some dangerous but less commonly researched types that targets ancillary services of the energy industry such as linear deception attack [69], replay attack [70] as well as resonance attack [71]. Overall, FDIA and DoS attacks are the two most regularly seen in this domain, and they have been proven lethal to a wide range of smart power system elements. For the scope of this review journal, we put the highest emphasis on two popular types of cyberattacks: False Data Injection Attack (FDIA) and DoS (DoS).

1) FDIA

The term ‘‘false data injection attack’’ in the smart grid domain describes the situation in which an adversary breaches sensor readings in such a way that undetected errors are introduced into calculations of state variables and values. Thus, the attacker can interfere with the state estimation processes and deceive the network operator [72]. The FDIA can have a variety of outcomes depending on the intruder’s objective, including errors in locational marginal prices (LMP) for illegal market profits, energy theft, and physical destruction through the network. FDIA can have an impact on the LMP by confusing the state estimation process, which then inadvertently involves the contingency analysis processes [73].

- Physical-based FDIA: This type of attack typically targets monitoring, control, and security devices. Several possibilities for this type of attack can be seen in [74], which discusses the various equipment access levels. FDIA could be implemented in any processor-based device by modifying the firmware of the remote terminal units (RTU). Even though the number of devices that are vulnerable to this type of attacked is somewhat limited, physical-based FDIA can still cause catastrophic consequences in the cyber-physical system, especially in smart grid and microgrid.
- Cyber-based FDIA [75]: These are the attacks in which the adversary penetrates either the control system or the associated applications (also known as the process layer), such as prediction, estimation, economic dispatch, energy trading, and so on. Even though this type is cyber-based, its target is still the operation and services of the system and can be initiated through physical as well as communication modules unlike malware insertion whose targets are computer software system and system database.

2) DoS

DoS attacks target electronic maneuvers and routing protocols, cramming communication channels and causing delays. As a result, a DoS attack can limit legitimate users’ access to services and resources by flooding the communication network with excessive traffic [76]. However, it is easy to defend the system against regular DoS by blocking the attacking site if the source of the attack is available and can be located. On the other hand, the Distributed DoS (DDoS) attack is a more extreme type of DoS attack in which a large number of hosts attack a victim site at the same time [77]. DDoS attackers plan their attacks in advance by exploiting a common vulnerability to compromise multiple hosts across the communication system. Then, they use all compromised hosts to flood the victim site. Regarding inverter-based smart power system, DoS can disrupt communication between the control system and all ‘‘agents’’ within a system, causing delay in distributed control framework for microgrid and can potentially paralyze communication between smart power electronics in smart grid. Broadly speaking, DDoS attacks can be classified into three specific types:

- Volume-based DDoS [78]: Volume-based DDoS attacks are specifically designed to flood not only internal networks but also even centralized DDoS scrubbing centers with massive amounts of anomalous traffic. This type of DDoS attacks often tries to eat up bandwidth within the target network/service or between it and the rest of the cyber-physical system. Famous volumetric DDoS attacks are User Datagram Protocol (UDP) flood, Internet Control Message Protocol ICMP) flood, IP/ICMP Fragmentation, IPsec flood and Reflection Amplication Attacks.
- Protocol DDoS [79]: Protocol DDoS attacks take full advantage of flaws in internet communication protocols to cause DoS attacks. Because many of these protocols are widely used, changing their functionality is complex, difficult, and time-consuming. Furthermore, the inherent complexity of many protocols means that even when they are reconfigured to fix existing flaws, new weaknesses are frequently introduced, allowing for new types of protocol attacks. Protocol DDoS attacks often include SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more.
- Application Layer DDoS [80]: Application layer attacks, also known as Layer 7 (L7) DDoS attacks, are a special type of anomalous behavior aimed at infiltrating the OSI model’s ‘‘top’’ layer, which is where many popular internet requests like HTTP GET and HTTP POST take place. In comparison with network layer attacks such as DNS Amplification, these attacks are particularly effective because they consume server resources in addition to network resources. Application Layer DDoS attacks involve low-and-slow attacks, GET/POST floods as well as attacks that target Apache, Windows or OpenBSD vulnerabilities and even more.

Since Application Layer DDoS targets the front-end layer and ICT infrastructure such as server, website, operating systems, it is not relevant in the field of cyber-physical inverter-based power system and also not in the scope of our work. Volume-based DDoS and Protocol DDoS, on the other hand, pose significant threat to the cyber-physical grid and required a proper detection and mitigation method to ensure the resilience and safety of advanced energy system.

B. FOUNDATION OF CYBERSECURITY IN CPPS

According to previous research, the following cybersecurity research areas for CPPS have been identified: cyberattack risk modeling and mitigation, protection and control methodologies, security against coordinated cyber intrusions, the security feature of AMI infrastructure, as well as simulation models for the cyber-physical system. Regarding CPPS, cybersecurity research revolves around the analysis of detection, mitigation, and resilience methods against certain types of attacks. Attack prevention is the ability to prevent attacks on the system through risk assessment, while attack detection focuses mainly on the ability to recognize anomaly intrusion in both online and offline operations. Attack mitigation refers to the application of mitigation techniques to keep the system functioning without any disruption or degradation in the grid's performance, security, or stability. Furthermore, we also have a higher form of cybersecurity in the CPS, attack resilience, which is all about designing a smart control system that maintains the operational status at all costs even if an attack occurs. Overall, the fundamental goal of this field's cybersecurity research is to create a risk modeling framework that incorporates both physical and cyber dynamic behavior. The model can then be employed to determine the influence of a cyberattack on the power system in terms of load loss, stability issues, economic losses, and equipment failure. Based on the risk assessment above, the next step in our study is to review state-of-the-art defense algorithms created to protect the energy system against the two most popular types of cyberattacks in this field, FDIA, and DoS.

C. PREVENTION METHOD: SELF-SECURED INVERTER

t is more common to design detection and mitigation methods that apply at the control level to universally protect CPPS from malicious intrusions. Individually protecting each agent within the system using encryption measures does not tend to be effective since the synchronous update of all agents in that direction is required to achieve a great security performance for the system since even if one agent gets attacked and manipulated, the CPPS can be put at risk. However, with the development of science and technology, as well as the rise in demand for a fully functional smart grid, smart inverter technology is becoming cheaper over time and will soon be applied more frequently in the real world. Traditionally, a smart inverter is defined as a grid-interactive inverter that provides auxiliary services. However, more extensive functions such as self-governing, self-adapting, self-security, and self-healing will be necessary amid the rise in concern for a secured CPPS with renewable energy integration.

The ability to support the grid by offering autonomous auxiliary services or constructing microgrids by modulating grid voltage and frequency is regarded as the self-governing feature. To be specific, the self-governing features refer to the grid-supporting and grid-forming function of the smart inverter as well as its control techniques, which all have been discussed in previous sections. The self-adapting feature, on the other hand, is about seamless transition and islanding detection of microgrid, supervisory control using forecasting data, and adaptive stabilizers. The formation of an islanded microgrid may subject inverters to a weak grid condition. Therefore, the self-adapting feature is crucial for any modern smart inverter. However, the scope of this section is about the self-security feature and its healing capability against external malicious threats.

1) SELF-SECURITY FEATURE AND OPERATING REGION

Regarding communication standards, a communication network for smart inverters should be able to meet several criteria such as highly secure, high scalability, low latency, and good data rate [81]. Similar to the Distributed Energy Storage Systems demonstrated in previous sections, it is common for smart inverter systems to use the IEC 61850 standard as a platform for operation. In IEC 61850, the generic-object-oriented-substation-events (GOOSE) protocol is often utilized to transfer and receive data among intelligent electronic devices (IED) within a CPS. In contrast, the manufacturing-message-specification (MMS) protocol handles the real-time communication between the system operator and the IED system. Furthermore, the sample-measured-values (SMV) protocol is in charge of transferring digitized signals obtained from sensors and meters to the IED infrastructure. It is common knowledge that there is a delay in the processing and data package transmission between smart inverters, sensors, and the utility. Hence the performance of a centralized control framework in suppressing transient and fast dynamic phenomena will be limited. Cybercriminals can take advantage of such delay to inflict instability to the system [81]–[83]. Choosing the proper data transmission method is also vital for such a system. Available options are optical fiber, power line, cellular, wireless, etc. Even though wired communication techniques are typically more resistant to electromagnetic interference (EMI), they are less expandable than wireless communication methods. Nonetheless, wireless methods also suffer from complicated routing processes, impacting the data rate. In this manner, sparse communication technique, which only permits smart inverters to communicate with their nearby devices only, is often utilized to reduce complication and offer great scalability [84], [85].

Since the operation of the smart inverter can be improved by utilizing external data from the control center or even other agents in the system, the data packet exchange via a communication network either between inverters and the control center or among several inverters within the system can expose inverters to cyberattacks, and inadvertent human errors [86], [87]. As shown in Fig. 6, this problem can be solved by establishing a reference system that distinguishes a malicious setpoint from a regular one obtained from the power utility. One way to distinguish it is to use the Message

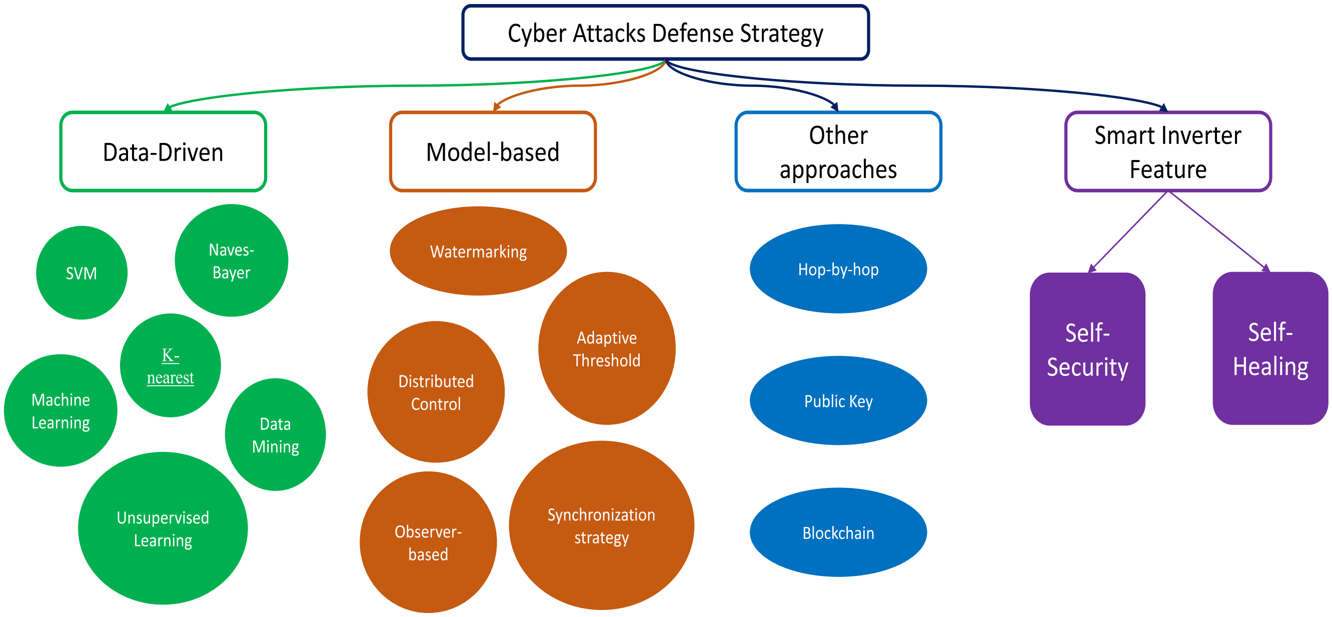

FIGURE 5. A quick summary of different type of detection and mitigation approaches.

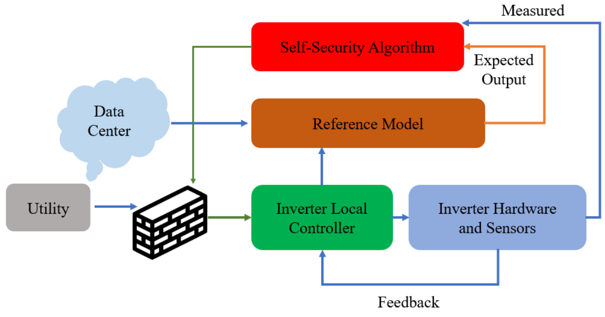

FIGURE 6. A model-reference way to examining and determining cyberattacks vs healthy utility supervisory control commands.

Authentication Code (MAC) methods in order to confirm whether the setpoint was manipulated or not. However, if attackers manage to hack the computer network that handles MAC, the smart inverter can still be compromised. There are some ways to mitigate these issues. One of the most popular ways is to utilize the operating region of the smart inverter. If an attacker modifies the inverter setpoints, the inverters can first assess the new setpoints by utilizing the reference mode. The smart inverter can decline to engage with those setpoints if the output deviates from the inverter's safe operating zone. Based on the foundation of this method, authors in [88] proposed a malicious setpoint detection method using the eighth order Butterworth lowpass filter. However, depending on the specific type of cyberattack, different methods can be developed to effectively protect the smart inverter from intrusion [89], [90].

It is important to note that the MAC and operating region of the smart inverter can do very well in protecting the inverter from FDIA in case attackers choose smart inverter as the point of initiation. However, the aforementioned techniques can not prevent DoS since the nature of DoS is not to alter the setpoint of the device but to flood the communication link with the massive amount of usually correct data. More preventative methods for DoS will be discussed in the following section.

2) FAULT-TOLERANT AND SELF-HEALING FEATURES

If a fault is diagnosed and isolated, the inverter, and thus the entire system, is expected to resume normal functioning as a sign of system reliability. In general, the diagnostics and isolation (D&I) technique are critical to prevent the problem from spreading and potentially having disastrous repercussions. Several ways are proposed to continue working in bad conditions, some of which include the installation of additional hardware and changes to the topology and/or modulation procedure [91], [92] at the device level. The idea of "redundancy" is used at this level to accomplish the fault tolerance characteristic. Fault-tolerant inverters are often classified as either non-redundant or redundant techniques [93]. Inverters utilizing non-redundant approaches must transition to a new control scheme after detecting an incipient problem in order to continue operating with a smaller amount of active devices. For non-redundant approaches, the key components, such as semiconductor devices, must also be overrated. Even in case an inverter remains functional after successfully isolating an internal fault, non-redundant approaches can result in highly unbalanced grid currents.

Redundant techniques, on the other hand, are often used for a two-level inverter with the integration of an auxiliary leg. In this scenario, the faulty leg must be separated, and also the auxiliary leg must be appropriately connected to the circuit. Each switch in these types of inverters has a fast-response overcurrent fuse to separate the device in the event of a short-circuit error. Once the device has been isolated, the faulty branch will behave as if it were an open circuit. Furthermore, the defection should be detected using an open-circuit fault detection method. Then, in order to integrate a device from the auxiliary into the circuit, the relevant switch should be set depending on the position of the fault. Despite the fact that two-level inverters are often employed in grid-tied implementation, modular multi-level inverters are often more tolerant of internal defects than two-level inverters [94]–[96]. In [97], the implementation of additional hardware is not included, and the proposed research exploited the redundancy of multi-level inverters to create fault tolerance, as an example of module-level fault tolerance. The general idea behind this is to overcome malfunctioning semiconductor switches, and the frequently unstable output voltage is governed by adjusting the modulation technique to account for a phase shift in the reference voltage and eventually provide balanced and stable line-to-line output voltages. Furthermore, there are also several other self-healing techniques applicable for multi-level inverters that should be taken into consideration, such as fundamental phase-shift compensation [98], [99], continuous self-healing techniques [96], sensor-per-source (SPS) algorithm as well as sensor-per-leg (SPL) algorithm [96]. Last but not least, to improve smart inverters, more thorough self-healing mechanisms and remedial actions can be adopted for modular battery-powered grid-forming inverters. With the combination of self-security and self-healing features, smart inverters can become resilient to cyberattacks.

D. PREVENTION METHOD: ENCRYPTION APPROACH

1) ENCRYPTION METHODS FOR FDIA AVOIDANCE

a: HOP-BY-HOP AUTHENTICATION

Even though this approach is proven to be applicable for FDIA prevention, its mechanism is not suitable for preventing DoS attacks since DoS can flood the communication among agents and jam the data transfer traffic from nodes to the base station [100].

b: PUBLIC KEY CRYPTOGRAPHY

Public key cryptography is another valuable solution for detecting cyber assaults in smart power systems, particularly FDIA. Cryptographic approaches are often utilized for Wireless Sensor Network (WSN). However, with the integration of smart metering devices and smart inverters with ICT features, such approaches are becoming more applicable than ever. In general, the Rivest – Shamir – Adleman (RSA), Elliptic Curve Cryptography (ECC) schemes, and public-key cryptography are popular cryptographic methods for data authentication, and FDIA rejection [101], [102]. Among the various public-key cryptography methods, the McEliece public-key system can effectively protect the integrity of smart grid data measurements while negating the influence of FDIA. The algorithm is based on how difficult it is to decode a standard linear code. A fault-correcting code with a known and powerful decryption method and the ability to fix errors is chosen to describe the private key. The McEliece system is generally formed by three different algorithms, including a probabilistic key generation algorithm that generates both a public and private key, a probabilistic encryption technique, and a deterministic decryption algorithm. Based on this foundation, the authors of [103] proposed an FDI attack prevention technique based on ensuring the integrity and availability of measurements at measurement units and during transmission to control center even in the presence of compromised units, which showed promising results. However, using such cryptographic approach entails some computational costs and should be taken into consideration.

c: TRUST-BASED APPROACHES

Another encryption method for inverter-based smart grid is the trust value mechanism, which has also been popular for its application in WSN, similar to the aforementioned cryptographic methods. In this approach, the difference between the attacker and the normal node is detected using the deployed hash algorithm. To identify the malevolent nodes, a model that evaluates trust is used. Using the hash algorithm [104], this technique assigns a unique identity to each sensor in the network. The cluster head then dynamically manages the sensor node's trust value with the help of the model that evaluates trust value. The cluster head establishes a trust threshold in order to detect malicious nodes. Once the malicious node has been identified, the cluster head notifies the management center and requests that the malicious node be removed. As a result, when a sensor node navigates to another cluster, the leader then returns the trust value to the management center. Eventually, the management center will respond to the leader of the cluster's queries. The trust value is regarded by the cluster leader as the initial trust value of the nodes in the investigated cluster. This method is expected to be a solution for FDIA prevention. In order to enhance the lifetime of the network and improve the packet delivery ratio, authors in [105] proposed a trust-based malicious node Detection and Routing (TMDR) technique in which the trust computation mechanism is utilized to calculate the trust value of every node in the network. The topic is further discussed in [106], in which the RSA algorithm is utilized in cooperation with routing techniques to achieve data integrity and data authentication as well as to optimize the energy consumption of nodes.

In general, for FDIA prevention, encryption methods, especially for the case of cryptographic approaches, are proven to have great benefits. However, the computational burden of such methods is still significant. Therefore, more research needs to be conducted to reduce energy consumption and computing cost and enhance the effectiveness, accuracy, and computing speed of the algorithm.

2) ENCRYPTION METHODS FOR DoS AVOIDANCE

The threat of DoS attack is the mass amount of packets sent to the system, not the packet's content itself, as described in previous sections. In the field of computer science, there are many proposed preventative approaches to tackle DoS, such as strengthening the data authentication [107] dividing the network resources into different classes of services [108], improving network and routing infrastructures, statistical monitoring network [109], [110] and congestion algorithms. In the context of the cyber-physical layer of the inverter-based smart grid, according to the scope of our study, authentication and encryption approaches are taken into consideration, with an example of the application of Advanced Encryption Standard (AES) algorithm as demonstrated in [111]. However, due to the computational load required for defense, such traditional cryptographic tools that can be used to prevent DoS and DDoS attacks may degrade service quality and even create an open opportunity for DoS attack [112]. In order to increase the reliability of encryption algorithms, puzzle-based mechanism are proposed. Puzzle-based defense mechanisms correct the mismatch between the cost to the attacker of generating a request and the cost to the server of handling a request by mandating a payment from each client in the manner of a puzzle solution [113]. Different puzzle-based schemes are developed for DoS prevention based on this general principle.

a: CLIENT PUZZLE SCHEME

In the client puzzle, a puzzle is generated by the server and has to be solved by the client. After solving the puzzle, the client then determines the latency of the file that must be retrieved from the server database. After that, the client encrypts the request and sends it to the server. The encryption and decryption are carried out using the AES algorithm. The server must decrypt the received request using the client's port number and IP address. The server encrypts the requested file before sending it. Finally, the file is delivered to the client, who decrypts the content and reads it. As a result, more reliable communication between server and client can be achieved, and active communications remain untouched even in the case of DDoS attacks. Its application in DoS prevention can be referred in [114].

b: TIME-LOCK PUZZLE SCHEME

A time-lock puzzle is a technique that a sender submits the solution to the message to be sent, effectively concealing it until the puzzle is solved. The initial objective is to make sure that a client could not decrypt a message until a certain amount of time had passed. The puzzles are developed to be non-parallelizable so that a client could not simply utilize more computing resources to solve the problem in less time. Utilizing the solution to a time-lock puzzle as the key to an encryption scheme would, on the surface, force anyone attempting to decrypt the message to conduct the computation for the amount of time it took to solve the puzzle. Overall, such non-parallelizability makes this scheme applicable for DoS prevention [115]. However, it is recommended not to use time-lock puzzles for DoS prevention due to the high cost of puzzle generation and verification at the server.

c: HASH-CHAIN PUZZLE SCHEME

Similar to the Time-lock puzzle, a hash-chain puzzle scheme is also a non-parallelizable approach. To prevent DDoS attacks, Authors in [116] introduced the hash-chain-reversal puzzles. Non-parallelizability is a property of this puzzle since inverting the digest i in the chain could not begin until the inversion of the digest i+1 is accomplished. However, construction and confirmation of the puzzle solution on the server are incredibly costly. Furthermore, using a shorter digest length hash function does not always guarantee the intended computation cost at the client-side, whereas abusing a longer hash length tends to make the puzzle impractical to solve in a decent amount of time.

Another worth-mentioning hash chain puzzle applicable for DoS prevention has been proposed by authors of [117]. Even though this hash-chain puzzle is also non-parallelizable, it has a number of flaws since the cost of building and verifying puzzles on the server is relatively high, and sending a puzzle to a client consumes much bandwidth.

Despite various research in this area, the common disadvantage of the encryption-based prevention method for DoS is the high computational burden, which is critical and should be tackled to ensure the approach's applicability in the real world.

E. DETECTION AND MITIGATION METHODS

1) DETECTION & MITIGATION METHODS FOR FDIA

a: DATA DRIVEN APPROACH

When the modeling of a power system is not available or feasible to construct, the historical operation log could be utilized for data-driven detection and mitigation strategy. The flexibility provided by data-driven methods means that more types of power systems could be equipped with cybersecurity features. The trade-off, however, resides in more considerable computing power for training data and the accuracy erosion of the system under changing grid conditions. Efforts are being made to decrease the resource needed.

b: DATA-DRIVEN APPROACH: SUPERVISED LEARNING METHODS

According to [118], the data-driven approach in CPS consists of machine learning branches such as neural network, Naives-Bayer, and support vector method. However, in our study, based on how data is used to detect cyberattacks in smart grids, these algorithms can be divided into intelligent algorithms, which use cutting-edge machine learning technology and are highly efficient but have a high computational burden, and traditional data mining algorithms, which are lighter and preferable for certain applications. In general, the application of data-driven methods is very flexible since it only needs measurement data of voltage and current sent from smart power electronics, smart meters, and sensors; other additional data types can also come in handy for this method.

In general, machine learning has the capability to perform various complicated tasks, including the detection of cyber-attacks based on the data collected from the system. Machine learning-based detection algorithms can often be classified into supervised learning, and unsupervised learning, each of them has its benefits and drawbacks at the moment. Supervised learning is a process that data needs to be labeled before being used for the learning process of the machine and is often widely popular among researchers to detect malicious intrusion into the power system.

The most straightforward supervised learning technique, linear regression, has been utilized to detect the infamous FDIA in the smart meter system [119]. This approach compares the difference between the dependent scalar variable and the independent variable using the least square approach. A cyberattack, especially FDIA, can be found if the measurement vector does not meet the requirement of the linear model generated from the trained set of data.

Naives-Bayes classifier (NBC) is also one of the more simple probabilistic classifiers utilized to detect cyberattacks in the smart grid. This method is not well-known in cybersecurity, even though its application can be found in various classification problems. In [120], NBC was used in conjunction with Hybrid Bernoulli Random Set (HBRS) and Kullback-Leibler to detect intrusion effectively and securely estimate the system state in a cluster-based network structure in which multiple cluster-heads obtain information from external sensors via non-secure links and transfer processed information neighbor-wise through the use of secure links. The same idea can be applied to a network of smart inverters.

Another frequently used technique is Support Vector Machine (SVM). Given a series of training examples, each labeled as belonging to one of two categories; an SVM training method constructs a model that assigns future examples to one of the two categories, resulting in a non-probabilistic binary linear classifier. SVM maps training examples to points in space in order to widen the distance between the two categories as much as possible. New examples are then mapped into that same space and projected to belong to one of the categories based on which side of the gap they land on. SVM is a famous and elegant linear non-probabilistic classifier frequently and a class of machine learning based on the boundaries of two parallel hyperplanes. In [121], a multi-class support vector machine (MSVM) was employed for anomaly classification and localization. The suggested method makes use of statistical features derived from measurements to optimize the learning of a pair of MSVM classifiers. In order to compare the performance, the mean absolute percentage error is utilized, and the results are evaluated by comparing them to artificial neural networks, Naives-Bayes classification. Multi-class support vector machine (MSVM) detected the majority of the anomalies and has been proven to have much higher efficiency than either Naives Bayes or Artificial Neural Network. However, the primary downside of this strategy is the selection of the kernel function and the requirement for memory and substantial CPU time during the training phase.

Furthermore, in [122], the well-known classification technique K-nearest neighbor (KNN) was used to detect FDIA. In such research, the KNN classifier is trained to utilize normal and abnormal data generated by the simulation studies of normal and stressed conditions. KNN employs the features space during the training phase to store the instances' locations and their class label. It determines the class of the sample, normal or stressed, in the test step by computing its neighborhood. This classification method has high computational efficiency, which is suitable for real-time applications. However, the dispersion and density of the prelabeled samples are the key disadvantages of this approach.

For a more complex and intensive detection of malicious signals, the neural network will be involved. Artificial neural networks (ANN), which are popular in computer science, were invented and used in classification, estimation, or approximating processes that rely heavily on many inputs and are typically unknown. Those very networks can have more than one hidden layer and feedback, and their output often varies depending on either the weighted sum of all the inputs and the activation function. The most recent yet interesting usage of ANN to detect cyberattacks can be viewed in [123], in which the model predictive control/artificial neural network (MPC/ANN) defense strategy was proposed. The role of MPC is to inject a certain amount of data into the system to quickly move the effect of FDIA and help the system heal. This research is the pioneer to utilize MPC to reduce the impact of a cyber-assault by utilizing the model predictive controller's quick operation characteristic and the non - linear mapping capability of ANNs.

Long-short Term Memory Network (LSTM), known for its state-of-the-art impact in the field of forecasting and predictive study, has recently been applied for cyberattack detection in [67]. Specifically, the authors of such study developed a hierarchical model of long short-term memory network to process raw data sets obtained from relevant CPS sensors and continuously monitor embedded signals in the data to identify and analyze the lethal time delay attack, which is famous for its exploitation of flaws in communication channels to cause potentially serious damage to the CPPS. The method reaches the accuracy of 92% in the power plant control system and 94% for automatic generation control (AGC), which are higher than the accuracy of methods like KNN or Random Forests. However, this approach can complicate the system if being applied to the system with multiple control signals. Therefore, it requires serious consideration when implementing on complex industrial system.

c: DATA-DRIVEN APPROACH: UNSUPERVISED LEARNING METHODS

The main disadvantages of supervised learning methods are the demand for extensive learning as well as the labeled data. Unsupervised learning, unlike supervised learning, is the process of delivering unlabeled data to the machine to find hidden classification schemes and patterns. Thus, the machine's job is to divide the data points into classes according to the hidden features of the data points. We can detect cyberattacks in intelligent grids as those with different classes other than the typical data classes. In this regard, several unsupervised learning algorithms have been utilized in detecting malicious attacks in power electronic-based smart power systems.

One of the unsupervised learning algorithm, isolation forest, finds anomalies based on the assumption that their numbers are few and the data points' outstanding values. The algorithm isolates abnormal data by randomly selecting a data point and seeking other objects with similar properties. This type of branching means that abnormal objects are isolated closer to the 'root' of the process, and abnormalities can be measured by the distance from the top isolated object. Performance of four outlier algorithms (Isolation Forest, Robust Covariance Estimation, Local Outlier Factor, and One-Class SVM) against FDIA in IEEE 14-bus system is compared to one another in [124], with a reduced-dimension dataset using Principal Component Analysis (PCA) for feature extraction. A similar application [125] helps detect stealthy FDIA on four IEEE distribution network models. But in [126], compared with supervised learning algorithms, Isolation Forest shows worse performance with the higher false-positive rate on a reduced-dimension dataset which includes both natural contingencies and attack events.

Deep belief network (DBN) is a fast and efficient deep learning algorithm that consists of stacked Restricted Boltzmann machines (RBMs) trained greedy layer-wise. DBN parameter optimization is a frequent research topic. In [127], a variety of DBN parameter optimization techniques and LSTM are compared under partial and complete knowledge FDIA, DoS, and Reconnaissance attacks on industrial control systems. In [128], the backpropagation algorithm handles fine-tuning DBN, which achieves superior accuracy and running time than SVM under different simulated IEEE testcases and proportions of tampered data in sample sets.

The Hidden Markov Model, a statistical Markov model in which the system being represented is believed to be a Markov process with unobserved (hidden) states, has also lately been adopted for false data detection. In [129], authors propose a novel Hidden Markov model (HMM) based method for detecting FDIA in advance metering infrastructures (AMI), which are typically seen in inverter-based power systems. In this method, HMM is trained using historical meter data in offline mode, and the Vitberi algorithm devises its hidden state. However, this research assumed that the profile does not change, which is not realistic for all the cases. In addition, [130] presents an IDS architecture that employs machine learning methods such as the HMM in a multi-layer manner. The multi-layer technique can be extended beyond two layers to effectively capture multi-phase attacks across a more considerable time duration. HMMs can convert dissimilar digital events across both protocols and platforms into enforceable information, with lower layers identifying discrete events and higher layers identifying new states resulting from multi-phase events in the lower layers. This concept is up-and-coming in this field, but its full potential requires more investigation.

d: DATA-DRIVEN APPROACH: TRADITIONAL DATA MINING

The approach of detecting patterns in massive data sets without using machine learning is known as traditional data mining. We can use traditional data mining algorithms to process variable data measurements obtained from a particular system to deduce the data's hidden attributes or patterns. Therefore, the data mining approach can detect cyberattacks very effectively by mining the dataset just like the intelligent approach but without the additional computational cost. Despite the fact that data-mining methodologies require historical data sets, the low computational complexity of data mining algorithms after training is a significant plus for detecting cyberattacks in smart grids. As a result, several real-time online experimental tests were carried out and validated. Data-mining based method can be listed as hoeffding adaptive trees [131], causal event graph [132], common path mining (CPM) [133] and signal temporal logic (STL) [134].

Among those methods, Signal Temporal Logic (STL) is the most commonly researched and utilized to detect FDIA. STL method was proposed in [134] to detect FDIA by comparing the DC voltage and DC current with the predefined upper and lower boundary known as the STL requirements. Any infringement of STL requirements indicates the existence of a cyber intrusion. The authors utilized the Breach toolbox from MATLAB to compute the robustness degree and mine the necessary value. The results were verified using the DC Microgrid composed of 24 DC-DC converters implemented in a controller-hardware-in-loop (CHIL) system using the Typhoon HIL603. Based on that foundation, a defense mechanism based on time-frequency logic formalism and continuous wavelet transform was proposed in [135] by the same authors, featuring the parameter synthesis methods similar to the 2019 studies. This data mining approach shows great effectiveness and potential for application in the real system.

In general,the traditional data mining approach is lighter, cheaper to implement, and requires less computing power than the machine learning counterpart. Even though its effectiveness and scalability are somewhat limited, this approach can still be applied in small-scale power systems such as microgrids or as a supportive anomaly detection system in parallel with the more complicated one mentioned in not only the intelligent approach section above but also the model-based methods described in the following section of our study.

e: MODEL-BASED APPROACH

Model-based methods, along with data-driven methods, are two traditional ways to detect and mitigate FDIA [136]. As the penetration of renewable energy increases on the distribution level, defense strategy for not only DER-based microgrids but distribution networks becomes a significant concern due to the decentralized nature and the vulnerability of power electronics under frequency and voltage instability [137]. These systems may interact with each other or be considered in isolation, which further complicates and fragments cybersecurity issues.

f: MODEL-BASED APPROACH: DISTRIBUTED WATERMARKING

To discern a genuine signal from a malicious one, the control signal could be combined with a verification signal similar to a watermark on a document. The approach does not require a central process to facilitate the detection scheme, but it requires dynamic modeling of system components to identify the watermarked signal correctly. In [138], by injecting a time-varying perturbation on top of the operational signal for the DC actuator, or in other words, ''watermarking'' the signal, replay attack could be prevented. The simulation of a 4-bus DC microgrid on MATLAB shows that the estimator could detect replay attacks through residual signal disturbance while the effect of the watermark signal is minimal under spectral analysis. In [139], distributed watermark shows its effectiveness against destabilizing attack on economic droop control used in high renewable penetration microgrids, with the strategy formulation taken from author's prior work for transmission grid model [39], showing a degree of adaptability among different scenarios.

g: MODEL-BASED APPROACH: GRAPH THEORY APPROACH

Graph theory approach aims to reduce redundancy links between each renewable source while allowing the network to remain connected and thus work coherently when under attack.

In [140], a resilient, economical control scheme is used to correct the economic droop coefficient of microgrid while under communication disruption and delays. The graph theory approach is adaptive in the sense that it allows the operator to set the number r of potential malicious neighboring distributed generators (DGs), and as in this case, retain control stability up to $r+1$. The strategy is verified by MATLAB simulation for 4-DG and 20-DG microgrids.

h: MODEL-BASED APPROACH: CROSS-LAYER CONTROL

Under a cooperated attack that simultaneously compromises all inverters in the microgrid, cross-layer resilient control is a more viable solution. In [141], a hidden control network is proposed for redundant communication links in case the main communication network has been infiltrated. The hidden layer utilizes Internet-level technology to secure the hidden network while it is also unintelligible in terms of useful information. The parallel control layer in [142] helps strengthen the original control network layer. Unlike the hidden network approach, these control layers depend on each other's state, and disabling either could lead to failure. Stability of the control strategy under normal working conditions is considered as there could be interference with the introduction of another parallel, always-on control mechanism. In PSCAD/EMTDC simulation, the grid frequency is restored during the DoS attack, and the 12-bus DER microgrid is able to withstand a combined FDI – DoS attack.

The success of hidden layer strategy lies in how well such layer is kept from attacker's knowledge or away from their ability to manipulate system's signal [143], and thus fall prey to an adversary with knowledge or access to the power system.

i: MODEL-BASED APPROACH: OBSERVER-BASED STRATEGY

The observer-based defense intends to support the state estimator in detecting and discarding bad data. It is an approach with various solutions for different resilient targets.

In [143], the resiliency of islanded AC microgrid against stealth probing is achieved by taking untampered signals from safe inverters to substitute for those of compromised inverters. The indication of attacked inverters is based on an adaptive threshold that relies on the mismatching of reference active power between inverters. The distributed control strategy is effective up to all but one uncompromised inverter (n-1 resiliency). The method is verified by the DRT platform simulating a four-bus AC microgrid under FDIA. In [127], the finite-time observer-based controller is incorporated with a trust-based algorithm to detect the existence of attack and discard according to tampered information, and a confidence algorithm to locate the source of the attack and restore its value to the reference one. The simulated strategy on a 5-DG AC microgrid is tested to restore voltage and frequency after link and node attacks.

The Kullback-Leibler divergence is a statistical check for comparing the received information with Gaussian distribution in [144]. Based on the aforementioned check, the DER controller calculates their individual trust factor and the local neighbouring trust factor, which means there is also a consensus step. Demonstration with 34-bus IEEE system simulation and hardware-in-the-loop (HIL) testing proves the effectiveness of the strategy.

Sliding mode observer is demonstrated to contain a variety of attacks on DER in [145]. By reconstructing the attack signal, the original information could be retrieved by signal compensation. This control technique does not require additional measurements other than those used by DER controllers. It could keep delivered power at reference level under both FDIA and DoS.

2) DETECTION & MITIGATION METHODS FOR DoS

Most papers consider a DoS attack that completely paralysed the communication link or sensors, leading to omission of that link from the communication network or static return value from sensors if it employs zero-order hold. Although DoS is more detectable than FDIA, a combined FDIA and DoS attack may cause great difficulty to any control or mitigation strategy due to the inability to manipulate DoS-isolated agents on the immediate control layer. Detection methods improve system awareness of the operator, which then take the necessary step to secure the network and block out malicious signals, while resilient control strategy aims to avoid the DoS-affected section and maintain connection to isolated agents through another mean. All of the following papers propose strategies that work with both FDIA and DoS.

a: DATA-DRIVEN METHODS

In [146], the anomaly detector for WAMPAC uses variational mode decomposition for feature extraction of PMU measurement, which is then used to train the decision tree algorithm to detect and classify events, either FDIA, DoS attacks, line fault or malicious tripping. The time-frequency logic formalism and continuous wavelet transform method in [135] can detect FDIA, DoS attack along with physical fault in both AC and DC microgrid, even with noisy data input. In [121], MSVM can detect FDIA, DoS and determine the compromised agent also with noisy data, regardless of transient condition. While method in [135] can detect anomalies in both AC and DC microgrids, the ability to differentiate transient conditions is not mentioned. The method in [121] is only implemented on the AC microgrid. Both of these methods lack an anomaly classifier which could provide greater system awareness to microgrid operator.

b: MODEL-BASED METHODS

Patel *et al.* [147] presents a dynamic switching method that utilizes alternative measuring points in the transmission system to the wide-area damping controller in case the original ones are compromised by a DoS attack. Zhou *et al.* [142] proposes an auxiliary control network that provides redundant communication links in AC microgrid. Under normal operation, the control strategy remains stable since the auxiliary network does not interfere with the main network. The sliding mode controller for the DER system in [145] is resilient to DoS attack and can compensate for the lack of grid voltage measurement of two phases through signal reconstruction.

A compilation of various worth-mentioning defense strategies along with corresponding vulnerabilities they tackle can be seen in Table 3.

IV. A REVIEW OF CONDUCTING EXPERIMENT AND TESTBED FOR SMART POWER SYSTEM

In this part, we review and follow a step-by-step approach to validate and assess defense strategy. Firstly, the environment for simulation is determined. Most prominent grid configurations are IEEE testcases, consisted of simplified real power network on both transmission and distribution scales. These premade test case can be modified to include renewable energy, or modified into microgrid model, especially with distribution testcases like IEEE 34-bus [135]. Microgrid model with a cooperative inverter control can also be connected in mesh, and the topology is described in Laplacian matrix. Secondly, it must be determined how the attack is conducted and what effect it has on the system. Thirdly, an appropriate testbed is chosen, based on the simulation requirement.

A. SELECTION OF POWER SYSTEM TESTCASE

For transmission or distribution system simulation, testcase can be chosen from a list of pre-made, simplified model of a real electrical network. The selection of pre-made testcases offer several advantages. There is no need to model and test a new test case before implementing the research [161]. Also, a standardised testcase means that the model is used by previous researches, making it a benchmark to compare results of different cybersecurity strategies. Alternatively, the testcase can be modified to integrate DER sources and smart grid technologies such as PMU, voltage regulator, etc. to test control strategies against cyberattack on renewable-rich grid [153].

However, the topology and configuration of a microgrid varies by papers. Microgrids have to abide by interconnection standard, which means that there are requirements on voltage, frequency and their variation threshold. Nevertheless, standards for microgrid varies between countries and for specific applications, leading to a wide range of microgrid configuration in cybersecurity studies [162]. Encountered testcases are either created from the ground up [142] or modified from a standard distribution testcase [141]. For example, in [142], the custom 12-bus microgrid testcase is divided by switch at the middle of the system to test the microgrid distributed control strategy under FDIA and reconfiguration of the system.

The N-agent microgrid configuration appears in many papers with AC/DC islanded microgrid testcase. It consists of various DG - load subsystems, which are connected to one another through short transmission line (resistor-inductor model) in case of AC microgrid or pure resistive line in case of DC microgrid. [143] and [163] provide general mathematical formulations for AC and DC N-agent microgrids, respectively.

A compilation of encountered testcases, along with their modifications, notably with DER elements, is presented in Table 4.

B. CREATING CYBERATTACK SCENARIO

A list of cyberattack simulation is presented in Table 5. An attack on the physical layer is defined as parameters manipulation on local controller, while attack on cyber layer is defined as manipulation on communication lines or centralised controller parameters. In case of co-simulation platform, the targeted parameters can be manipulated on their respective simulating software, and the effect of the attack can cascade to other layers, corresponding with other softwares. Aspects such as length of attack, details of injected data, attacked components, etc. depend on individual studies.

C. CHOOSING SUITABLE TESTBED

Based on smart power systems models, a comprehensive testbed includes the physical and communication layers. The physical layer consists of hardware like load models, DG, power electronics, and transmission lines. Devices in the physical layer can be represented by a mathematical model that approximates their physical dynamics. Signals such as

TABLE 3. A compilation of various reviewed defense strategies in Section III with corresponding vulnerabilities demonstrated in Section II.

Vulnerability	Strategies	Classification			Against FDIA	Against DoS	Citation
		Preventive	*Model-based Detection*	*Data-driven Detection*			
Attack on Inverters and DER Controller	Signal Temporal Logic			✓	✓	✓	[135], [136]
	Perturbation-based Diagnosis		✓		✓		[139]
	Dynamic Watermarking		✓		✓		[140]
	Sliding-mode observer		✓		✓	✓	[147], [150]
Attack on Communication System	Multi-class Support Vector Machine			✓	✓	✓	[122]
	MPC/ANN-based Strategy			✓	✓		[124]
	Isolation Forest			✓	✓		[126], [127]
	Distributed Watermarking		✓		✓		[139]
	Resilient Economic Control		✓		✓		[142]
	Cross-layer Distributed Control		✓		✓	✓	[144]
	Kullback-Leibler Divergence		✓		✓	✓	[146]
Attack on WAMPAC application	Common Path Mining			✓	✓	✓	[134]
	Variation mode decomposition			✓	✓	✓	[148]
Attack from IoT devices connected to inverter-based smart grid	Evolutionary Deep Belief Network			✓	✓		[128]
Attack on Metering Infrastructure	K-Nearest Neighbour			✓	✓		[123]
	Short-lived Pattern			✓	✓		[151]
	Hoeffding Adaptive Tree			✓	✓		[132]
	Linear Regression			✓	✓		[120]
	Local Matrix Reconstruction			✓	✓		[152]
	Hidden Markov Model			✓	✓		[130]
	Eighth-order Butterworth Lowpass Filter	✓			✓	✓	[89]
	Hop-by-hop Authentication	✓			✓		[101]
	Public Key Cryptography	✓			✓		[102]–[104]
	Trust-based Approaches	✓			✓		[105]–[107]
	Puzzle-based Mechanisms	✓				✓	[114]–[116], [118]
Attack on Energy Management System	Isolation Forest			✓	✓		[125]
	Deep Belief Network			✓	✓		[129]

TABLE 4. Compilation of cybersecurity testcase configuration.

	Test System	Type of power system	Voltage (kV)	AC/DC	No. of Buses	Used in	Note
Pre-made testcases	IEEE 13	Distribution	4.16	AC	13	[153]	Modified with addition of PV DERs
						[154]	Modified with addition of BESS DERs
	IEEE 14	Transmission	13.8, 18, 69	AC	14	[125]	
	IEEE 34	Distribution	4.16, 24.9	AC	34	[136], [143], [146]	Modified into microgrid with DERs
						[155]	Modified with addition of PV-ESS DERs
	IEEE 69	Distribution	12.66	AC	69	[137]	Modified with addition of DERs
Custom testcases	N-agent microgrid	Microgrid	Varied, usually low-voltage	AC and DC	Varied	[156], [157]	3-bus, 4-DG AC microgrid
						[158]	11-bus, 9-DG, 2-energy-storage AC microgrid
						[139]	4-bus, 4-DG DC microgrid
	12-bus microgrid	Microgrid	N/A	AC	12	[144]	Includes grid coupling point and reconfiguration switch
	Residential grid cluster	Distribution	0.12	AC	17	[159]	Radial distribution network with residential PV
	Distribution grid breakout microgrid	Microgrid	10.5	AC	7	[138]	Includes PV, ESS DERs with synchronous generators

voltage, current, etc., measured by agents in the grid, are transmitted via the communication layer implemented by software based on a protocol standard. There are inherent problems when trying to integrate physical and communications layers into a co-simulation testbed, prominently the interface of a discrete system (cyber) with an analog system

TABLE 5. Compilation of attack simulation method.

System	Attack category	Affected layer	Affected element	Attack simulation method	References
DC microgrid	Stealthy FDIA	Physical	DG's output voltage and current	Parameter manipulation	[145]
	Time delay	Cyber	Data latency	Time delay loops	[145]
	Coordinated FDIA	Physical + Cyber	DG's output current	Parameter manipulation	[124]
	DoS	Cyber	Measurement from neighbouring DGs	Switch off communication link	[160]
	Replay attack	Cyber	Measurement from neighbouring DGs	Previously recorded measurements are sent to neighbouring DGs, real-time measurements are discarded	[139]
AC microgrid	FDIA	Physical	DG's frequency	Parameter manipulation	[161]
	DoS	Cyber	Measurement from neighbouring DGs, control signal to DGs	Switch off communication link	[144]
Distribution network	DERMS hijacking	Cyber	Control commands to DER	Modify control commands in DERMS simulator	[162]
	FDIA	Physical	Differential voltage measurement	Real-time measurement replaced with historical measurement	[137]
	DoS	Cyber	Sensor measurement	Block new measurement for set amount of time	[149]

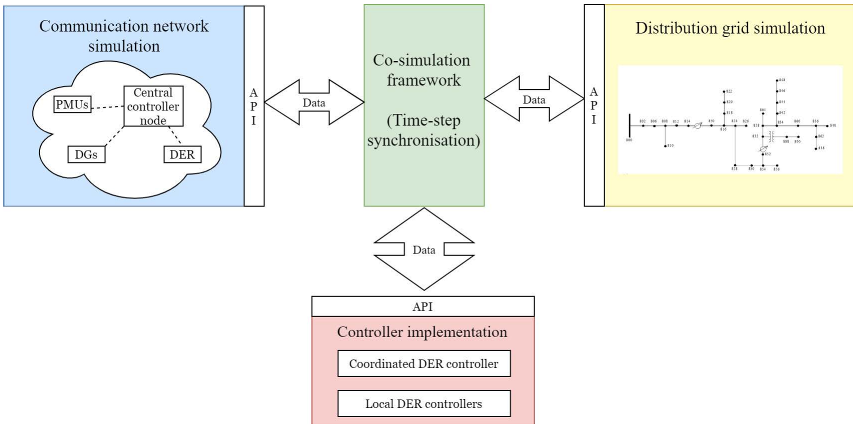
Communication network simulation
PMUs
Central controller node
DGs
DER
API
Data
Co-simulation framework
(Time-step synchronisation)
Data
API
Distribution grid simulation
Data
API
Controller implementation
Coordinated DER controller
Local DER controllers

FIGURE 7. Co-simulation environment diagram of a distribution grid with grid-connected DER [153].

(physical) [164], and implementation of network protocol between these two layers [165]. Researchers can also choose to demonstrate large scale test on simulation platform before experimentally validate their strategies on HIL testbed [144].

Reviewed articles implemented their strategies on either microgrid or smart power systems. The test platforms have been classified into the following groups [8]:

1) NON-REAL-TIME SIMULATOR

A significant number of researchers use simulation platforms for their studies. This could be attributed to the disruptive nature of cyberattacks on power equipment and simulation platform being more economical [166], [167]. Simulation is the process of creating and running a computer model that is based on a real-world system. A simulation platform provides functions to monitor the state of and collect data from simulated system [168]. Creating a simulator demands the mathematical description of individual components in the system. The entire system can be simulated using software that supports and provides power system device's models [154]. In cybersecurity study, common simulation time scale ranges from fractions of a second to hours, which is suitable for studying transient dynamics and load changes in the power system [169]. When the dynamics of the communication layer are not important to the defense strategy, information exchanges between agents in the network can be shared instantaneously [170]. For co-simulation, the communication layer can also be simulated on different software and coupled with the physical layer's simulation through an API. Works must be done to ensure that the solver between these two layers is compatible and time-synchronized [171]. A dedicated software for coupling two simulators could ensure that the simulations between such software are synchronized, and the data transfer is performed smoothly.

MATLAB/Simulink is widely used for demonstrating resilient control [127], [154], [156], [170], [172], mitigation strategy [144], [151] and detection method [138]. This is due

TABLE 6. Comparison between power simulation software.

Name	Licence	API support for co-simulation	Notable feature
MATLAB	Commercial licence with student discount	Yes	Official and third-party add-ons
PSCAD/EMTDC	Trialware with commercial licence	Yes	FORTRAN supported programming
DigSilent POWERFACTORY	Commercial licence with student discount	Yes	Specialised power grid study features
GridLab-D	Free and open-source	Yes	Support for economical calculation

TABLE 7. Comparison between communication simulation software [174].

Name	Frequent simulation	Advantage	Disadvantage
Opnet	General network	Complete and multi-level network library	Proprietary software
OMNET++	General network	Easily expandable model, GUI-based, open-source	Dual language use
NS-2	Internet simulation	Rich internet model base, open-source, expandable with C++ and OTcl	Lacking modelling tools and components, dual language use
NS-3	IP-based network	Expandable and better integration with C++ and python, efficient	Dual language use, limited time-sensitive network support
Simulink	General network	Visual modelling, data processing capabilities, expandable model	Limited time-sensitive network support

to the multidisciplinary nature of the software, which helps with the flexibility of implementing control strategy through the included high-level language [135], [170]. In [173], the distributed control strategy for the islanded microgrid is tested on the PSCAD/EMTDC platform. In [151], DigSilent POWERFACTORY handles the physical layer simulation, while MATLAB acts as a DER communication network. In [160], the distribution grid simulator GridLab-D is coupled with the distributed network simulator NS-3 through HELICS co-simulation software. In [153], the Functional Mockup Interface standard is implemented in Python for a co-simulation platform combining MATLAB for designing and running the controller, EMTP for power system simulation, and NS-3 for handling the communication layer. The platform is used in evaluating the resiliency of the DER coordinated control and communication system. A list of power grid simulation software can be found in Table 6, as well as communication software in Table 7.

2) DIGITAL REAL-TIME TESTBEDS (DRT)

Power system is inherently a real-time, continuous system. Emulation of subsections in the system can be off-loaded to specialized hardware created to study power system dynamics. In contrast to non-real-time simulations, these devices not only act as virtual systems whose communication data and characteristics match that of the real power network but also achieve real-time simulation speed. While they come in the form of HIL, they may be more comprehensive with the inclusion of a dedicated software tool-chain [175] and support for interfacing with simulation softwares to leverage the existing features in these software [123]. API is included as part of the solution to facilitate the integration of other hardware and software, such as data acquisition and actuator.

The heart of DRT is a specialized computer with a conventional microprocessor for real-time computation of power system models and FPGA for extensive I/O functions. Hardware capabilities such as the computational capacity of PC-grade processors, I/O support, connectivity mediums, and software features such as compatibility with third-party simulation software, library support, and convenient features are essential features to consider. In [176], MATLAB/Simulink software acts as an interface to the dSPACE 1103 inverter controller, and the inverter output is connected to the NHR 9410 regenerative power grid simulator. In [177] and [143], the DC microgrid is controlled by the DRT platform with the same interfacing method. In [178], the fallback control for the renewable-rich islanded microgrid is implemented as the EMS on MATLAB, while the microgrid is simulated on the OPAL-RT system and communicate with the simulated EMS through an internal TCP/IP connection.

Some DRT testbeds adopt a CHIL configuration for increased configurability. In [141], the AC microgrids are modeled on the Typhoon HIL 604, and an Ethernet network of dSPACE DS 1202 MicroLabBoxes handles the distributed control. In [144], Raspberry Pi modules simulate individual DG while the network layer is implemented on OPAL-RT.

3) HARDWARE

A large part of the hardware-based testbed is actual equipment used on the real system, such as power inverters and monitoring devices. The system is usually practical enough for uses outside of scholarly interest. The higher financial burden and low flexibility are trade-offs for the improved accuracy these systems bring, which means such systems are hard to come by in cyber-physical security analysis. Khan *et al.* [167] simulated the power-electronic-rich distribution system through four grid-following inverters. In [179], a push-pull DC-DC converter in a PV system is reserved for implementing a control strategy to mitigate sensor and actuator attacks.

4) ASSESSMENT AND RECOMMENDATION

For the non-real-time simulation platform, the architectural difference can lead to different execution times. Platform that supports compiled languages is much better optimized for simulating large and computation-heavy systems, but the interactive and user-friendly features of the GUI-based interface is a significant advantage as well [180].

PSCAD/EMTDC supports Fortran compiler, MATLAB can be programmed with its high-level language and C, and both have a GUI interface for model creation. As a multi-domain package that sees widespread application in institutional education, MATLAB/Simulink offers free learning resources, third-party support, and extensions by leveraging its community. While user-created cases can be picked up from the shared resource library, it is not guaranteed to work, does not have a warranty, and may cause even more frustration and loss of time to correct the model. Power system analysis software such as PSCAD/EMTDC and POWERFACTORY provides more specialized features to power grid operators, but their learning resources are limited. Gridlab-D application centers around renewable energy presence on the grid. Thus it is suitable for DER vulnerability and economical dispatch research. Gridlab-D may work as a distribution grid component in a co-simulation platform [160]. More comparison can be found in Table 8.

In real-time simulation, the model accuracy between different manufacturers is not a significant concern [181]. Instead, the features and compatibility are major key points for comparison between brands, whereas, in a brand's line-up, researchers need to consider price-performance trade-off when choosing a solution. Access to a hardware system could be a significant step up from digital simulation, providing the ability to validate the defense model under the most realistic situation possible. Hardware platforms are a valuable validation method for authors who have access to them [182]. Papers such as [179] and [167] indicate that dedicated hardware testbed is a feasible approach for modeling small-scale microgrids. For other cases, building cybersecurity test case from simulator and DRT are more desirable due to superior flexibility and reasonable modeling accuracy.

V. CHALLENGES AND FUTURE DIRECTION

A. THE TREND OF CYBER-PHYSICAL-SOCIAL SYSTEM IN THE ENERGY SECTOR

Conventionally, power system analysis is predicated on the premise that the major energy supply and end-use energy consumption are both unchanging and totally controllable. However, this boundary condition will be difficult to hold in the future when the rapid injection of renewable energy, raising in impact of social behavior as well as the evolve of electricity market and regulations all can affect and alter the energy sector in one way or another. According to [183], the energy systems have an opportunity to evolve from cyber-physical system to cyber-physical-social system (CPSS). Apart from the existing technologies that have been supporting the CPPS in recent decades such as ICT infrastructures or decentralized controllers, it is important for a system to be a CPSS to have the coordination of various additional factors such as social, economic and human behaviour, which entails a wide range of massive data sets with hidden relationships in the complex economic, technological, social, and environmental elements. Human behaviour is considered to be the most crucial of them all since the current trend of technological development is to achieve maximum customer satisfaction and be able to cope with the uncertainty of human comportment. An example of this trend in power system research is the demand response topic as many researchers have been investigating the way to develop a proper demand response algorithm that integrate not only the target for maximum profits for both side participating but also the target for maximum customer satisfaction. Furthermore, in order to enable the CPS to evolve to the CPSS, it is also essential to develop in the Internet of Things, Big Data, Cloud Computing, Network Systems incorporating cognitive science, social psychology, and political science. Since human behavior, individual privacy, and data security all have a significant impact on the objectives of power system operation and optimization, these additional challenges must be taken into consideration in future power system monitoring and control studies. This will not be an easy journey, but a rather necessary one for humanity to achieve a better and more optimal power system that can handle all external disturbances that occur both nature-origin and man-made alike.

B. RESILIENCE PHILOSOPHY IN SMART POWER SYSTEM

Cyber resilience refers to CPPS's ability to plan for, respond to, and recover from cyber threats. It is crucial for a critical system like a power grid to be able to adapt to ever-changing conditions and withstand and recover quickly from disruptions in order to enhance the power quality as well as system reliability. In addition to power system resilience, cyber system resilience should be taken into account while establishing control and operation techniques and planning strategies to improve electric grid resilience against physical and cyber catastrophes. However, a universally accepted definition of power system resilience, metrics, and methodologies, as well as a one-size-fits-all resilience solution for power systems, have not been available in the energy sector yet [184], making this topic very attractive for researchers to pursue. The next step for research in resiliency for smart power systems should be the monitoring and control functions that consider future trends pertaining to the resilience of cyber-physical microgrids and integrate all socioeconomic aspects possible in order to achieve a fully resilient cyber-physical-social intelligent power system. Furthermore, the standardization of the resilience concept should also be promoted and investigated.

C. EXISTING CHALLENGES, UNSOLVED PROBLEMS AND NEXT STEPS

In order to achieve the future of cyber resilient power systems, several challenges in the field need to be tackled. Firstly, uncertainties in system parameters, modeling, observations, and the dynamic characteristics of smart grids, with various states and operating circumstances, are identified as obstacles for CPPS research and should be considered in the future. A considerable proportion of published papers in power system security is related to the model-based cyberattack

TABLE 8. Taxonomy of existing cybersecurity testbed.

Type of grid	Attack method	Implemented controller	Grid simulation	Communication protocol	Dedicated communication simulation?	Dedicated controller simulation?	References
AC microgrid	FDIA	Distributed secondary control	MATLAB/Simulink	N/A	No	No	[156]
	FDIA	Distributed secondary controller	PSCAD/EMTDC	N/A	No	No	[176]
	FDIA	Hierarchical economic controller	MATLAB/Simulink	Ethernet	TrueTime2.0 (MATLAB/Simulink toolbox)	No	[142]
	DoS	Distributed reactive power sharing control	MATLAB/Simulink	N/A	No	No	[190]
	FDIA	Decentralised cooperative controller	OPAL-RT	N/A	No	No	[124]
	DoS	EMS with fallback control for ESS	OPAL-RT	Internet Protocol	No	MATLAB for EMS, NI-cRIO digital controller for fallback controller	[181]
	FDIA	Distributed secondary control	OPAL-RT	UDP	Raspberry Pi for each inverter	Raspberry Pi for each inverter	[146]
DC microgrid	Replay attack	Hierarchical controller	MATLAB/Simulink	N/A	No	No	[139]
	FDIA	Distributed EMS	Microgrid with controllable DC source and load	N/A	No (through controller hardware)	dSPACE MicroLabBox DS1202	[145]
Distribution grid with grid-connected inverters	FDIA	DER management system	GridLAB-D	DNP3	openDNP3	No	[162]
	FDIA	DER coordinated control system	EMTP	UDP	NS-3	MATLAB/Simulink	[155]
	FDIA, DoS	DMS	DigSilent POWERFACTORY	Open Platform Communications (OPC)	MATLAB/Simulink (OPC server)	No (through DigSilent POWERFACTORY)	[153]
	FDIA	Smart inverter primary controller	Powerflex 755 three-phase inverter; NHR 9410 power grid emulator	N/A	No	dSPACE 1103	[179]
PV system	FDIA	DC-DC push-pull converter controller	Test on converter	N/A	No	No	[182]

🟩 Software 🟨 DRT 🟥 Hardware

detection approaches, which often require accurate model information to develop the proper detection index. The existence of uncertainties can ultimately reduce the reliability of the detection algorithm. It is proposed that future research in smart grid in general and cybersecurity, in particular, should focus more on the model-free approach, either through the means of data-driven detection algorithm or advanced state estimation that can evaluate the state of the system regardless of system dynamics.

Another challenge for power system security is the lack of research interest in the hybrid AC-DC smart grid/microgrid. In a hybrid microgrid, the amount of vulnerability points for cyber exploitation has the potential to rise dramatically since the cyber-physical system now features not only inverter-based generation sources and inverter-based electrical devices but also synchronous generators and various AC-based appliances, therefore, complicating the task for modeling, control strategy development, and detection algorithm design. Moreover, the control strategy for the hybrid grid, in addition to protecting their respective voltage regions, needs to consider AC-DC interlinking problem [185].

Although not so directly relevant from a technical point of view but still extremely necessary for the future development of this research direction, the true definition for ‘‘CPSG’’ has yet to be decided internationally and officially, making it difficult for policymakers around the world to develop a synchronized smart grid roadmap as well as regulations and policies regarding cybersecurity. Consequently, it is essential to investigate and develop a standardized architecture, framework, and technological standard for the smart grid, laying the foundation for more appropriate security policies and cyberattack countermeasures to be proposed and developed.

Economic analysis is also vital for cybersecurity research. Estimating the cost of the cyberattack on CPPS from device-level to national-level is crucial for any scheme design that is applicable in the real world. It can be observed that economic analysis for cyber-physical energy system security is a research topic that is yet to mature since the number of researches that analyze the economic benefit of its proposed security method is extremely limited, resulting in the fact that most of those researches are not ready to be applicable in real power system. It is highly recommended that future researches integrate the economic analysis to increase the applicability and practicality of methodologies.

Last but not least, a standardized model for the microgrid is still lacking, and there is no universally accepted architecture, making it inconvenient for researchers to test their security algorithm. For the convenience of simulation, researchers in the field of cyber-physical smart grids usually use microgrids as their test system, as can be seen on various papers cited in the above sections. Even though it is well known that the standard microgrid architecture is the CERTS Microgrid Concept [186], such architecture is not widely adopted by researchers in this field, and people tend to reconfigure by themselves the IEEE power system model of either 9-bus, 34-bus, or beyond, leading to the heterogeneity of the experimental models. This inconsistency can lead to difficulty in comparative study and performance evaluation between methods and can potentially discourage people from entering the field. Therefore, developing a streamlined experimental procedure, model and testbed is definitely the next important step in this field.

D. ARTIFICIAL INTELLIGENCE AND BLOCKCHAIN: THE RISING STARS

Artificial intelligence is among the most concerned topics in the computer science community nowadays, with hundreds of publications and new inventions being published every day from all around the world. Its potential and application can bring significant benefits to almost all industries, so the implementation of AI will inevitably occur in the energy sector. Traditionally, artificial intelligence algorithms, especially deep learning, are often utilized for prediction and forecasting purposes. Authors in [188], for example, demonstrate the utilization of numerical method and deep learning to forecast the I-V characteristic of PV modules. The ability to forecast future events is a potent tool for power system operation since grid operators can use it to predict future scenarios, which will help them prepare better. Furthermore, deep learning can also be used to detect and recognize cyber anomalies based on the training of past data sets, as demonstrated in previous sections. In general, the capability of AI to detect advanced cyberattacks is still limited in terms of efficiency compared to other model-based approaches. However, due to the constant development of the field, artificial intelligence has great potential in power system cybersecurity, thus requiring further research and implementation of more intelligent AI algorithms to increase the detection capability of the power system against malicious attacks.

Moreover, the capability of AI is not limited to only detection or prediction task. Reinforcement learning, known for its application in the robotic field, has the potential to be applied in the multi-agent smart microgrid with smart meters, smart converters, and smart sensors. The ability to ‘‘learn’’ in real-time and deal with the cyberattack when such an attack occurs is one of the most valuable qualities of a top cybersecurity expert and what artificial intelligence is expected to be capable of. This research direction is yet to mature; therefore, it brings many opportunities for young researchers to participate in.

Along with the development of AI, Blockchain is also one of the most trendy topics that can be found nowadays. As illustrated in the previous section, Blockchain is highly secure and can be an excellent solution for not only the cybersecurity issue in the energy sector but also the way the sector works as well. Blockchain technology streamlines the entire asset management and payment process by offering an autonomous trade life cycle. All participants are granted access to similar data about a transaction, eliminating the demand for intermediaries while ensuring openness and good transactional data management. Cryptography, one of the major products of blockchain technology, has the potential to change the way our economy and trading work, which will result in a significant impact in several industries such as healthcare, government, CPG, retail, travel, and hospitality. In the context that the power grid in the energy sector is moving towards the form of cyber-physical-social system with a deep tie with economy and human behavior, blockchain technology can bring benefits that we might not even be able to imagine just yet. From our point of view, there are two research directions regarding the utilization of Blockchain in energy systems that should be considered. One direction is the application of Blockchain in the Peer-to-Peer (P2P) electricity market. It is essential to conduct scientific research to develop either new blockchain technology or market architecture with cryptography to ensure secured transaction and energy trading in an interconnected smart grid. The second direction is to employ Blockchain to guard the data transmission between components within a critical microgrid system, applicable for military bases, aircraft carriers, data centers, or financial towns. The cybersecurity industry is like a chess game; every time a scientist develops a new defense scheme for a particular system, a cybercriminal will always try to exploit such research's weaknesses and infiltrate the said system. Blockchain, in particular, has been the target for hackers for many years due to its popularity. Hence, scientific research to enhance the security of blockchain-based systems and Blockchain itself is indispensable.

With the unpredictable development of science and technology in recent years, it might be impossible to precisely predict the right path and what lies ahead, especially in the energy industry, which might change the fastest in upcoming decades. Nevertheless, with diligence and effort in scientific research, the dream of a fully resilient, highly secured cyber-physical-social power system with high electricity quality will not be just wishful thinking.

VI. CONCLUSION

Cybersecurity is one of the most concerned topics in the field of smart power systems. Due to the rapid development of information technology nowadays, there has been much interest in research studies on CPPS modeling, simulation, and analysis. This paper presents an all-inclusive review of the architecture and vulnerabilities of inverter-based power systems with deep integration of DER systems and smart power electronics. Furthermore, the state of development of several defense strategies and an overview of testbed and simulation tools along with appropriate recommendations have been demonstrated. Regarding defense strategy, not only state-of-the-art data-driven and model-based methods are reviewed, but our work also takes a deep dive into the self-security technology of smart inverters and also other approaches such as cryptography and authentication-based methods. Moreover, the established control systems for the smart power system have been evaluated, with the unresolved concerns identified. Research trends, issues in securing the networked smart grid, and new possible technology for future smart grid cybersecurity are also discussed.

Uncertainties and standardization issues, the continuous growth of smart grid technology, the boom of renewable energy, the lack of in-depth cyber-economic analysis, and the lack of standardization of microgrid model for convenient research are all supposed to be critical challenges in this field and should be taken into consideration. Resiliency philosophy, artificial intelligence, blockchain, and quantum computer are the industry's rising stars and have the potential to bring significant benefits to scientific research in this field, requiring additional attention. With the collective revision of state-of-the-art solutions that have previously been investigated, this study is expected to lay the foundation for the development of other related studies in the near future.

This work can also be expanded even further by analyzing the vulnerabilities of the inverter-based power system more mathematically with specific simulation results to systematically benchmark each vulnerability possible in the system and rank them according to the threat level and chance of occurrence, which can bring convenience for the analysis and selection of scientific topics for upcoming studies.

ACKNOWLEDGMENT

The authors wish to show their appreciation to members of 100% Renewable Energy Laboratory (100RE Lab), Hanoi University of Science and Technology (HUST), for the ongoing support during the drafting of this study, also special thanks to Hoang Nhat for his help in designing and drawing beautiful figures for this journal and Le Ngoc Dung for his help in data analysis and classification of types of cyberattack.

REFERENCES

[1] T. Klaus, C. Vollmer, K. Lehmann, K. Müschen, R. Albert, M. Bade, T. Charissé, F. Eckermann, R. Herbener, U. Kaulfersch, G. Knoche, K. Kuhnhenn, C. Lohse, C. Loreck, U. Lorenz, B. Lünenbürger, M. Memmler, C. Mordziol, A. Ostermeier, and B. Westermann, "2050 energy target: 100% renewable electricity supply," Federal Environ. Agency Germany, Dessau-Roßlau, Germany, Tech. Rep., Jul. 2010.

[2] T. V. Vu, B. L. H. Nguyen, Z. Cheng, M.-Y. Chow, and B. Zhang, "Cyber-physical microgrids: Toward future resilient communities," *IEEE Ind. Electron. Mag.*, vol. 14, no. 3, pp. 4–17, Sep. 2020.

[3] S. Gu, X. Du, Y. Shi, Y. Wu, P. Sun, and H.-M. Tai, "Power control for grid-connected converter to comply with safety operation limits during grid faults," in *Proc. IEEE Energy Convers. Congr. Expo. (ECCE)*, Sep. 2016, pp. 1–5.

[4] L. Wei, A. I. Sarwat, W. Saad, and S. Biswas, "Stochastic games for power grid protection against coordinated cyber-physical attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 684–694, Mar. 2018.

[5] S. Sahoo, T. Dragicevic, and F. Blaabjerg, "Cyber security in control of grid-tied power electronic converters—Challenges and vulnerabilities," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 5, pp. 5326–5340, Oct. 2021.

[6] J. H. Hong, C.-C. Liu, and M. Govindarasu, "Integrated anomaly detection for cyber security of the substations," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1643–1653, Jul. 2014.

[7] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Surv.*, vol. 41, pp. 1–58, Jul. 2009.

[8] M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, "A survey on smart grid cyber-physical system testbeds," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 446–464, 1st Quart., 2017.

[9] Y. Jiang, S. Yin, and O. Kaynak, "Data-driven monitoring and safety control of industrial cyber-physical systems: Basics and beyond," *IEEE Access*, vol. 6, pp. 47374–47384, 2018.

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

[11] H. Cui, F. Li, and K. Tomsovic, "Cyber-physical system testbed for power system monitoring and wide-area control verification," *IET Energy Syst. Integr.*, vol. 2, no. 1, pp. 32–39, Mar. 2020.

[12] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-physical power system (CPPS): A review on modeling, simulation, and analysis with cyber security applications," *IEEE Access*, vol. 8, pp. 151019–151064, 2020.

[13] M. Amin, F. F. M. El-Sousy, G. A. A. Aziz, K. Gaber, and O. A. Mohammed, "CPS attacks mitigation approaches on power electronic systems with security challenges for smart grid applications: A review," *IEEE Access*, vol. 9, pp. 38571–38601, 2021.

[14] 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.

[15] J. Qi, A. Hahn, X. Lu, J. Wang, and C.-C. Liu, "Cybersecurity for distributed energy resources and smart inverters," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 1, no. 1, pp. 28–39, 2016.

[16] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[17] A. J. M. Milne, A. Beckmann, and P. Kumar, "Cyber-physical trust systems driven by blockchain," *IEEE Access*, vol. 8, pp. 66423–66437, 2020.

[18] A. Ovalle, G. Ramos, S. Bacha, A. Hably, and A. Rumeau, "Decentralized control of voltage source converters in microgrids based on the application of instantaneous power theory," *IEEE Trans. Ind. Electron.*, vol. 62, no. 2, pp. 1152–1162, Feb. 2014.

[19] I. Serban and C. Marinescu, "Control strategy of three-phase battery energy storage systems for frequency support in microgrids and with uninterrupted supply of local loads," *IEEE Trans. Power Electron.*, vol. 29, no. 9, pp. 5010–5020, Sep. 2014.

[20] R. Jadeja, A. Ved, T. A. Trivedi, and G. Khanduja, "Control of power electronic converters in AC microgrid," in *Microgrid Architectures, Control and Protection Methods*. Berlin, Germany: Springer, 2020.

[21] *IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources With Associated Electric Power Systems Interfaces–Amendment 1: To Provide More Flexibility for Adoption of Abnormal Operating Performance Category III*, IEEE Standard 1547a-2020 (Amendment to IEEE Std 1547-2018), 2020, pp. 1–16.

[22] B. Palmintier, R. Broderick, B. Mather, M. Coddington, K. Baker, F. Ding, M. Reno, M. Lave, and A. Bharatkumar, "On the path to sunshot: Emerging issues and challenges in integrating solar with the distribution system," Nat. Renew. Energy Lab., Washington, DC, USA, Tech. Rep. NREL/TP5D00-65331, May 2016.

[23] M. Ahmed, R. Bhattarai, S. J. Hossain, S. Abdelrazek, and S. Kamalasadan, "Coordinated voltage control strategy for voltage regulators and voltage source converters integrated distribution system," *IEEE Trans. Ind. Appl.*, vol. 55, no. 4, pp. 4235–4246, Jul./Aug. 2019.

[24] T. O. Olowu, S. Dharmasena, H. Jafari, and A. Sarwat, "Investigation of false data injection attacks on smart inverter settings," in *Proc. IEEE CyberPELS (CyberPELS)*, Oct. 2020, pp. 1–6.

[25] J. Yaghoobi, N. Mithulananthan, and T. K. Saha, "Dynamic voltage stability of distribution system with a high penetration of rooftop PV units," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2015, pp. 1–5.

[26] S. Maharjan, A. M. Khambadkone, and J.-X. Xu, "Probing the impact of reduced DC capacitor size in variable speed drive loads on voltage stability of the distribution network at high PV penetration," in *Proc. IEEE Innov. Smart Grid Technol.-Asia (ISGT Asia)*, May 2018, pp. 220–225.

[27] S. Maharjan, A. M. Khambadkone, and J. C.-H. Peng, "Integration of centralized and local voltage control scheme in distribution network to reduce the operation of mechanically switched devices," in *Proc. IEEE Milan PowerTech*, Jun. 2019, pp. 1–6.

[28] P.-Y. Chen, S.-M. Cheng, and K.-C. Chen, "Smart attacks in smart grid communication networks," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 24–29, Aug. 2012.

[29] S. D. Roy and S. Debbarma, "Detection and mitigation of cyber-attacks on AGC systems of low inertia power grid," *IEEE Syst. J.*, vol. 14, no. 2, pp. 2023–2031, Jun. 2020.

[30] L. Che, X. Liu, and Z. Li, "Mitigating false data attacks induced overloads using a corrective dispatch scheme," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3081–3091, May 2019.

[31] Y. Chen, S. Huang, F. Liu, Z. Wang, and X. Sun, "Evaluation of reinforcement learning-based false data injection attack to automatic voltage control," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2158–2169, Mar. 2019.

[32] K. Jhala, B. Natarajan, A. Pahwa, and H. Wu, "Stability of transactive energy market-based power distribution system under data integrity attack," *IEEE Trans. Ind. Informat.*, vol. 15, no. 10, pp. 5541–5550, Oct. 2019.

[33] P. Li, Y. Liu, H. Xin, and X. Jiang, "A robust distributed economic dispatch strategy of virtual power plant under cyber-attacks," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4343–4352, Oct. 2018.

[34] A. Ameli, A. Hooshyar, E. F. El-Saadany, and A. M. Youssef, "Attack detection and identification for automatic generation control systems," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4760–4774, Sep. 2018.

[35] G. Clarke, D. Reynders, and E. Wright, "4—Preview of DNP3," in *Practical Modern SCADA Protocols*, G. Clarke, D. Reynders, and E. Wright, Eds. Oxford, U.K.: Newnes, 2003, pp. 66–72.

[36] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[37] A. Ameli, A. Hooshyar, A. H. Yazdavar, E. F. El-Saadany, and A. Youssef, "Attack detection for load frequency control systems using stochastic unknown input estimators," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 10, pp. 2575–2590, Oct. 2018.

[38] 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.

[39] T. Huang, B. Satchidanandan, P. R. Kumar, and L. Xie, "An online detection framework for cyber attacks on automatic generation control," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6816–6827, Nov. 2018.

[40] R. Tan, H. H. Nguyen, E. Y. S. Foo, D. K. Y. Yau, Z. Kalbarczyk, R. K. Iyer, and H. B. Gooi, "Modeling and mitigating impact of false data injection attacks on automatic generation control," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 7, pp. 1609–1624, Jul. 2017.

[41] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of Things security: A top-down survey," *Comput. Netw.*, vol. 141, pp. 199–221, Aug. 2018.

[42] A. Mosenia and N. K. Jha, "A comprehensive study of security of Internet-of-Things," *IEEE Trans. Emerg. Topics Comput.*, vol. 5, no. 4, pp. 586–602, Dec. 2017.

[43] F. Ahmad, A. Adnane, V. Franqueira, F. Kurugollu, and L. Liu, "Man-in-the-middle attacks in vehicular ad-hoc networks: Evaluating the impact of Attackers' strategies," *Sensors*, vol. 18, no. 11, p. 4040, Nov. 2018.

[44] Y. Li, Y. Wang, M. Wu, and H. Li, "Replay attack and defense of electric vehicle charging on GB/T 27930-2015 communication protocol," *J. Comput. Commun.*, vol. 7, no. 12, pp. 20–30, 2019.

[45] N. Saxena, S. Grijalva, V. Chukwuka, and A. V. Vasilakos, "Network security and privacy challenges in smart vehicle-to-grid," *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 88–98, Aug. 2017.

[46] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber attack-resilient control for smart grid," in *Proc. IEEE PES Innov. Smart Grid Technol. (ISGT)*, Jan. 2012, pp. 1–3.

[47] M. Schukat, "Securing critical infrastructure," in *Proc. 10th Int. Conf. Digit. Technol.*, Jul. 2014, pp. 298–304.

[48] E. Luiijf, *Understanding Cyber Threats and Vulnerabilities*. Berlin, Germany: Springer, 2012, pp. 52–67.

[49] Y. Liu, "Wireless sensor network applications in smart grid: Recent trends and challenges," *Int. J. Distrib. Sensor Netw.*, vol. 8, no. 9, Sep. 2012, Art. no. 492819.

[50] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 99–107, Jun. 2010.

[51] P. Sakarindr and N. Ansari, "Security services in group communications over wireless infrastructure, mobile ad hoc, and wireless sensor networks," *IEEE Wireless Commun.*, vol. 14, no. 5, pp. 8–20, Oct. 2007.

[52] B. A. Akyol, H. Kirkham, S. L. Clements, and M. Hadley, "A survey of wireless communications for the electric power system," Pacific Northwest Nat. Lab., Richland, WA, USA, Tech. Rep. PNNL-19084, 2010.

[53] Z. Saad-Saoud, M. L. Lisboa, J. B. Ekanayake, N. Jenkins, and G. Strbac, ''Application of STATCOMs to wind farms,'' *IEE Proc.-Generat., Transmiss., Distrib.*, vol. 145, no. 5, pp. 511–516, Sep. 1998.

[54] S. Ahsan and A. Siddiqui, ''Dynamic compensation of real and reactive power in wind farms using STATCOM,'' *Perspectives Sci.*, vol. 8, pp. 519–521, Sep. 2016.

[55] L. Xu and P. Cartwright, ''Direct active and reactive power control of DFIG for wind energy generation,'' *IEEE Trans. Energy Convers.*, vol. 21, no. 3, pp. 750–758, Sep. 2006.

[56] F. Blaabjerg and Z. Chen, *Power Electronics for Modern Wind Turbines*. Williston, VT, USA: Morgan & Claypool, 2006.

[57] J. Ye, A. Giani, A. Elasser, S. K. Mazumder, C. Farnell, H. A. Mantooth, T. Kim, J. Liu, B. Chen, G.-S. Seo, W. Song, M. D. R. Greidanus, S. Sahoo, F. Blaabjerg, J. Zhang, L. Guo, B. Ahn, M. B. Shadmand, N. R. Gajanur, and M. A. Abbaszada, ''A review of cyber-physical security for photovoltaic systems,'' *IEEE J. Emerg. Sel. Topics Power Electron.*, early access, Sep. 10, 2021, doi: 10.1109/JESTPE.2021.3111728.

[58] V. V. G. Krishnan, R. Liu, A. Askerman, A. Srivastava, D. Bakken, and P. Panciatici, ''Resilient cyber infrastructure for the minimum wind curtailment remedial control scheme,'' *IEEE Trans. Ind. Appl.*, vol. 55, pp. 943–953, Jan. 2019.

[59] P. Srikantha and D. Kundur, ''Hierarchical signal processing for tractable power flow management in electric grid networks,'' *IEEE Trans. Signal Inf. Process. Netw.*, vol. 5, no. 1, pp. 86–99, Mar. 2019.

[60] R. Palma-Behnke, C. Benavides, F. Lanas, B. Severino, L. Reyes, J. Llanos, and D. Sáez, ''A microgrid energy management system based on the rolling horizon strategy,'' *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 996–1006, Jun. 2013.

[61] P. Siano, C. Cecati, H. Yu, and J. Kolbusz, ''Real time operation of smart grids via FCN networks and optimal power flow,'' *IEEE Trans. Ind. Informat.*, vol. 8, no. 4, pp. 944–952, Nov. 2012.

[62] Q. Shafiee, S. Member, J. M. Guerrero, S. Member, and J. C. Vasquez, ''Distributed secondary control for islanded MicroGrids—A novel approach,'' *IEEE Trans. Power Electron.*, vol. 29, no. 2, pp. 1018–1031, Feb. 2014.

[63] C. Zhao, J. He, P. Cheng, and J. Chen, ''Analysis of consensus-based distributed economic dispatch under stealthy attacks,'' *IEEE Trans. Ind. Electron.*, vol. 64, no. 6, pp. 5107–5117, Jun. 2017.

[64] A. Teixeira, G. Dán, H. Sandberg, and K. H. Johansson, ''A cyber security study of a SCADA energy management system: Stealthy deception attacks on the state estimator,'' *IFAC Proc. Volumes*, vol. 44, no. 1, pp. 11271–11277, Jan. 2011.

[65] A. Huseinović, S. Mrdović, K. Bicakci, and S. Uludag, ''A survey of denial-of-service attacks and solutions in the smart grid,'' *IEEE Access*, vol. 8, pp. 177447–177470, 2020.

[66] E.-N.-S. Youssef and F. Labeau, ''False data injection attacks against state estimation in smart grids: Challenges and opportunities,'' in *Proc. IEEE Can. Conf. Electr. Comput. Eng. (CCECE)*, May 2018, pp. 1–5.

[67] P. Ganesh, X. Lou, Y. Chen, R. Tan, D. K. Y. Yau, D. Chen, and M. Winslett, ''Learning-based simultaneous detection and characterization of time delay attack in cyber-physical systems,'' *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3581–3593, Jul. 2021.

[68] K. Gai, M. Qiu, Z. Ming, H. Zhao, and L. Qiu, ''Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks,'' *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2431–2439, May 2017.

[69] C. Wang, J. Huang, D. Wang, and F. Li, ''A secure strategy for a cyber physical system with multi-sensor under linear deception attack,'' *J. Franklin Inst.*, vol. 358, no. 13, pp. 6666–6683, Sep. 2021.

[70] A. A. Elsaeidy, N. Jagannath, A. G. Sanchis, A. Jamalipour, and K. S. Munasinghe, ''Replay attack detection in smart cities using deep learning,'' *IEEE Access*, vol. 8, pp. 137825–137837, 2020.

[71] Y. Wu, Z. Wei, J. Weng, X. Li, and R. H. Deng, ''Resonance attacks on load frequency control of smart grids,'' *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4490–4502, Sep. 2018.

[72] B. Li, G. Xiao, R. Lu, R. Deng, and H. Bao, ''On feasibility and limitations of detecting false data injection attacks on power grid state estimation using D-FACTS devices,'' *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 854–864, Feb. 2020.

[73] M. M. N. Aboelwafa, K. G. Seddik, M. H. Eldefrawy, Y. Gadallah, and M. Gidlund, ''A machine-learning-based technique for false data injection attacks detection in industrial IoT,'' *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8462–8471, Sep. 2020.

[74] C. Konstantinou and M. Maniatakos, ''Hardware-layer intelligence collection for smart grid embedded systems,'' *J. Hardw. Syst. Secur.*, vol. 3, no. 2, pp. 132–146, Jun. 2019.

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

[76] X.-M. Zhang, Q.-L. Han, X. Ge, and L. Ding, ''Resilient control design based on a sampled-data model for a class of networked control systems under denial-of-service attacks,'' *IEEE Trans. Cybern.*, vol. 50, no. 8, pp. 3616–3626, Aug. 2020.

[77] A. Y. Nur and M. E. Tozal, ''Defending cyber-physical systems against DoS attacks,'' in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, May 2016, pp. 1–3.

[78] D. Ding, M. Savi, F. Pederzolli, M. Campanella, and D. Siracusa, ''In-network volumetric DDoS victim identification using programmable commodity switches,'' *IEEE Trans. Netw. Service Manage.*, vol. 18, no. 2, pp. 1191–1202, Jun. 2021.

[79] M. Dimolianis, A. Pavlidis, and V. Maglaris, ''SYN flood attack detection and mitigation using machine learning traffic classification and programmable data plane filtering,'' in *Proc. 24th Conf. Innov. Clouds, Internet Netw. Workshops (ICIN)*, Mar. 2021, pp. 126–133.

[80] K. S. Bhosale, M. Nenova, and G. Iliev, ''The distributed denial of service attacks (DDoS) prevention mechanisms on application layer,'' in *Proc. 13th Int. Conf. Adv. Technol., Syst. Services Telecommun. (TELSIKS)*, Oct. 2017, pp. 136–139.

[81] B. Arbab-Zavar, E. Palacios-Garcia, J. Vasquez, and J. Guerrero, ''Smart inverters for microgrid applications: A review,'' *Energies*, vol. 12, no. 5, p. 840, Mar. 2019.

[82] I. Serban, S. Céspedes, C. Marinescu, C. A. Azurdia-Meza, J. S. Gómez, and D. S. Hueichapan, ''Communication requirements in microgrids: A practical survey,'' *IEEE Access*, vol. 8, pp. 47694–47712, 2020.

[83] S. Kumar, S. Islam, and A. Jolfaei, ''Microgrid communications—Protocol and standard,'' in *Variability, Scalability and Stability of Microgrids*. Edison, NJ, USA: IET, Jul. 2019, ch. 9, pp. 291–326.

[84] X. Wu, C. Shen, and R. Iravani, ''A distributed, cooperative frequency and voltage control for microgrids,'' *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2764–2776, Jul. 2018.

[85] A. Bidram, A. Davoudi, and F. L. Lewis, ''A multiobjective distributed control framework for islanded AC microgrids,'' *IEEE Trans. Ind. Informat.*, vol. 10, no. 3, pp. 1785–1798, Aug. 2014.

[86] T. S. Ustun, ''Cybersecurity vulnerabilities of smart inverters and their impacts on power system operation,'' in *Proc. Int. Conf. Power Electron., Control Autom. (ICPECA)*, Nov. 2019, pp. 1–4.

[87] 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.

[88] T. Hossen, F. Sadeque, M. Gursoy, and B. Mirafzal, ''Self-secure inverters against malicious setpoints,'' in *Proc. IEEE Electric Power Energy Conf. (EPEC)*, Nov. 2020, pp. 1–6.

[89] S. Tan, J. M. Guerrero, P. Xie, R. Han, and J. C. Vasquez, ''Brief survey on attack detection methods for cyber-physical systems,'' *IEEE Syst. J.*, vol. 14, no. 4, pp. 5329–5339, Dec. 2020.

[90] D. Ding, Q.-L. Han, Y. Xiang, C. Ge, and X.-M. Zhang, ''A survey on security control and attack detection for industrial cyber-physical systems,'' *Neurocomputing*, vol. 275, pp. 1674–1683, Jan. 2018.

[91] W. Zhang, D. Xu, P. N. Enjeti, H. Li, J. T. Hawke, and H. S. Krishnamoorthy, ''Survey on fault-tolerant techniques for power electronic converters,'' *IEEE Trans. Power Electron.*, vol. 29, no. 12, pp. 6319–6331, Dec. 2014.

[92] P. Lezana, J. Pou, T. A. Meynard, J. Rodríguez, S. Ceballos, and F. Richardeau, ''Survey on fault operation on multilevel inverters,'' *IEEE Trans. Ind. Electron.*, vol. 57, no. 7, pp. 2207–2218, Jul. 2010.

[93] C. Cecati, A. O. D. Tommaso, F. Genduso, R. Miceli, and G. R. Galluzzo, ''Comprehensive modeling and experimental testing of fault detection and management of a nonredundant fault-tolerant VSI,'' *IEEE Trans. Ind. Electron.*, vol. 62, no. 6, pp. 3945–3954, Jun. 2015.

[94] B. Mirafzal, ''Survey of fault-tolerance techniques for three-phase voltage source inverters,'' *IEEE Trans. Ind. Electron.*, vol. 61, no. 10, pp. 5192–5202, Oct. 2014.

[95] H. Akagi, ''Classification, terminology, and application of the modular multilevel cascade converter (MMCC),'' in *Proc. Int. Power Electron. Conf. (ECCE ASIA)*, Jun. 2010, pp. 508–515.

[96] J. Lamb and B. Mirafzal, ''An adaptive SPWM technique for cascaded multilevel converters with time-variant DC sources,'' *IEEE Trans. Ind. Appl.*, vol. 52, no. 5, pp. 4146–4155, Sep./Oct. 2016.

[97] S. Li and L. Xu, ''Strategies of fault tolerant operation for three-level PWM inverters,'' *IEEE Trans. Power Electron.*, vol. 21, no. 4, pp. 933–940, Jul. 2006.

[98] P. W. Hammond, ''Enhancing the reliability of modular medium-voltage drives,'' *IEEE Trans. Ind. Electron.*, vol. 49, no. 5, pp. 948–954, Oct. 2002.

[99] P. Lezana and G. Ortiz, ''Extended operation of cascade multicell converters under fault condition,'' *IEEE Trans. Ind. Electron.*, vol. 56, no. 7, pp. 2697–2703, Jul. 2009.

[100] S. Zhu, S. Setia, S. Jajodia, and P. Ning, ''An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks,'' in *Proc. IEEE Symp. Secur. Privacy*, May 2004, pp. 259–271.

[101] H. Zhong, L. Shao, and J. Cui, ''A lightweight and secure data authentication scheme with privacy preservation for wireless sensor networks,'' in *Proc. Int. Conf. Netw. Netw. Appl. (NaNA)*, Jul. 2016, pp. 210–217.

[102] K. J. Choi and J.-I. Song, ''Investigation of feasible cryptographic algorithms for wireless sensor network,'' in *Proc. 8th Int. Conf. Adv. Commun. Technol.*, vol. 2, 2006, p. 1381.

[103] A. Abdallah and X. S. Shen, ''Efficient prevention technique for false data injection attack in smart grid,'' in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–6.

[104] W. Luo, W. Ma, and Q. Gao, ''A dynamic trust management system for wireless sensor networks,'' *Secur. Commun. Netw.*, vol. 9, no. 7, pp. 613–621, May 2016.

[105] M. R. Kumar, ''Trust-based malicious node detection and routing in wireless sensor networks,'' *Int. J. Emerg. Trends Sci. Technol.*, vol. 4, no. 8, pp. 5697–5702, Aug. 2017.

[106] B. Sreevidya and M. Rajesh, ''False data injection prevention in wireless sensor networks using node-level trust value computation,'' in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, Sep. 2018, pp. 2107–2112.

[107] C. Meadows, ''A cost-based framework for analysis of denial of service in networks,'' *J. Comput. Secur.*, vol. 9, nos. 1–2, pp. 143–164, Jan. 2001.

[108] J. Brustoloni, ''Protecting electronic commerce from distributed denial-of-service attacks,'' in *Proc. 11th Int. Conf. World Wide Web (WWW)*, 2002, pp. 553–561.

[109] S. Shyne, A. Hovak, and J. Riolo, ''Using active networking to thwart distributed denial of service attacks,'' in *Proc. IEEE Aerosp. Conf.*, vol. 3, Mar. 2001, pp. 3-1103–3-1108.

[110] D. Sterne, K. Djahandari, R. Balupari, W. La Cholter, B. Babson, B. Wilson, P. Narasimhan, A. Purtell, D. Schnackenberg, and S. Linden, ''Active network based DDoS defense,'' in *Proc. DARPA Act. Netw. Conf. Expo.*, 2002, pp. 193–203.

[111] Y. Javed, S. Khan, and A. Qahar, ''Preventing DoS attacks in IoT using AES,'' *J. Telecommun., Electron. Comput. Eng.*, vol. 9, nos. 3–11, pp. 55–60, Jan. 2018.

[112] A. Prakash, M. Satish, T. S. S. Bhargav, and N. Bhalaji, ''Detection and mitigation of denial of service attacks using stratified architecture,'' *Proc. Comput. Sci.*, vol. 87, pp. 275–280, Jan. 2016.

[113] A. Juels and J. Brainard, ''Client puzzles: A cryptographic countermeasure against connection depletion attacks,'' in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 1999. [Online]. Available: https://www.researchgate.net/publication/221655418_Client_Puzzles_A_Cryptographic_Countermeasure_Against_Connection_Depletion_Attacks

[114] T. Aura, P. Nikander, and J. Leiwo, ''DOS-resistant authentication with client puzzles,'' in *Proc. Int. Workshop Secur. Protocols*, vol. 2133, Jun. 2000, pp. 170–177.

[115] P. Tsang and S. Smith, ''Combating spam and denial-of-service attacks with trusted puzzle solvers,'' in *Proc. Int. Conf. Inf. Secur. Pract. Exper.*, vol. 4991, Apr. 2008, pp. 188–202.

[116] M. Ma, ''Mitigating denial of service attacks with password puzzles,'' in *Proc. Int. Conf. Inf. Technol., Coding Comput. (ITCC)*, vol. 2, 2005, pp. 621–626.

[117] B. Groza and D. Petrica, ''On chained cryptographic puzzles,'' 2006. [Online]. Available: https://www.semanticscholar.org/paper/On-Chained-Cryptographic-Puzzles-Groza-Petrica/ac8b958df1b1839a7f7478bea407bf2a2fc57ce5

[118] M. Kordestani and M. Saif, ''Observer-based attack detection and mitigation for cyberphysical systems: A review,'' *IEEE Syst., Man, Cybern. Mag.*, vol. 7, no. 2, pp. 35–60, Apr. 2021.

[119] S.-C. Yip, K. Wong, W.-P. Hew, M.-T. Gan, R. C.-W. Phan, and S.-W. Tan, ''Detection of energy theft and defective smart meters in smart grids using linear regression,'' *Int. J. Electr. Power Energy Syst.*, vol. 91, pp. 230–240, Oct. 2017.

[120] N. Forti, G. Battistelli, L. Chisci, S. Li, B. Wang, and B. Sinopoli, ''Distributed joint attack detection and secure state estimation,'' *IEEE Trans. Signal Inf. Process. Netw.*, vol. 4, no. 1, pp. 96–110, Mar. 2018.

[121] A. A. Khan, O. A. Beg, M. Alamaniotis, and S. Ahmed, ''Intelligent anomaly identification in cyber-physical inverter-based systems,'' *Electr. Power Syst. Res.*, vol. 193, Apr. 2021, Art. no. 107024.

[122] M. A. Hasnat and M. Rahnamay-Naeini, ''Detecting and locating cyber and physical stresses in smart grids using the k-nearest neighbour analysis of instantaneous correlation of states,'' *IET Smart Grid*, vol. 4, no. 3, pp. 307–320, Jun. 2021.

[123] M. R. Habibi, H. R. Baghaee, F. Blaabjerg, and T. Dragicevic, ''Secure MPC/ANN-based false data injection cyber-attack detection and mitigation in DC microgrids,'' *IEEE Syst. J.*, vol. 16, no. 1, pp. 1487–1498, Mar. 2022.

[124] C. Yang, Y. Wang, Y. Zhou, J. Ruan, and W. Liu, ''False data injection attacks detection in power system using machine learning method,'' *J. Comput. Commun.*, vol. 6, no. 11, pp. 276–286, 2018.

[125] S. Ahmed, Y. Lee, H. Seung-Ho, 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, Mar. 2019.

[126] R. Qi, C. Rasband, and J. Zheng, ''Detecting cyber attacks in smart grids using semi-supervised anomaly detection and deep representation learning,'' MPDI, Basel, Switzerland, 2021. [Online]. Available: https://www.mdpi.com/2078-2489/12/8/328

[127] K.-D. Lu, G.-Q. Zeng, X. Luo, J. Weng, W. Luo, and Y. Wu, ''Evolutionary deep belief network for cyber-attack detection in industrial automation and control system,'' *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7618–7627, Nov. 2021.

[128] L. Wei, D. Gao, and C. Luo, ''False data injection attacks detection with deep belief networks in smart grid,'' in *Proc. Chin. Automat. Congr. (CAC)*, Nov. 2018, pp. 2621–2625.

[129] B. Li, R. Lu, and G. Xiao, ''HMM-based fast detection of false data injections in advanced metering infrastructure,'' in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2017, pp. 1–6.

[130] W. Zegeye, R. Dean, and F. Moazzami, ''Multi-layer hidden Markov model based intrusion detection system,'' *Mach. Learn. Knowl. Extraction*, vol. 1, no. 1, pp. 265–286, Dec. 2018.

[131] U. Adhikari, T. H. Morris, and S. Pan, ''Applying Hoeffding adaptive trees for real-time cyber-power event and intrusion classification,'' *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4049–4060, Sep. 2018.

[132] U. Adhikari, T. H. Morris, and S. Pan, ''A causal event graph for cyber-power system events using synchrophasor,'' in *Proc. IEEE PES Gen. Meeting | Conf. Expo.*, Jul. 2014, pp. 1–5.

[133] S. Pan, T. Morris, and U. Adhikari, ''Classification of disturbances and cyber-attacks in power systems using heterogeneous time-synchronized data,'' *IEEE Trans. Ind. Informat.*, vol. 11, no. 3, pp. 650–662, Jun. 2015.

[134] O. A. Beg, L. V. Nguyen, T. T. Johnson, and A. Davoudi, ''Signal temporal logic-based attack detection in DC microgrids,'' *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3585–3595, Jul. 2019.

[135] O. A. Beg, L. V. Nguyen, T. T. Johnson, and A. Davoudi, ''Cyber-physical anomaly detection in microgrids using time-frequency logic formalism,'' *IEEE Access*, vol. 9, pp. 20012–20021, 2021.

[136] K. Jhala, P. Pradhan, and B. Natarajan, ''Perturbation-based diagnosis of false data injection attack using distributed energy resources,'' *IEEE Trans. Smart Grid*, vol. 12, no. 2, pp. 1589–1601, Mar. 2021.

[137] L. Xu, Q. Guo, Z. Wang, and H. Sun, ''Modeling of time-delayed distributed cyber-physical power systems for small-signal stability analysis,'' *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3425–3437, Jul. 2021.

[138] A. J. Gallo, M. S. Turan, F. Boem, G. Ferrari-Trecate, and T. Parisini, ''Distributed watermarking for secure control of microgrids under replay attacks,'' *IFAC-PapersOnLine*, vol. 51, no. 23, pp. 182–187, 2018.

[139] T. Huang, B. Wang, J. Ramos-Ruiz, P. Enjeti, P. R. Kumar, and L. Xie, ''Detection of cyber attacks in renewable-rich microgrids using dynamic watermarking,'' in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Aug. 2020, pp. 1–5.

[140] W. Zhang, T. Qian, X. Chen, K. Huang, W. Tang, and Q. Wu, ''Resilient economic control for distributed microgrids under false data injection attacks,'' *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 4435–4446, Sep. 2021.

[141] S. Zuo, O. A. Beg, F. L. Lewis, and A. Davoudi, ''Resilient networked AC microgrids under unbounded cyber attacks,'' *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 3785–3794, Sep. 2020.

[142] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, A. Abusorrah, L. Che, and X. Liu, ''Cross-layer distributed control strategy for cyber resilient microgrids,'' *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 3705–3717, Sep. 2021.

[143] S. Sahoo, T. Dragicevic, and F. Blaabjerg, ''Resilient operation of heterogeneous sources in cooperative DC microgrids,'' *IEEE Trans. Power Electron.*, vol. 35, no. 12, pp. 12601–12605, Dec. 2020.

[144] A. Mustafa, B. Poudel, A. Bidram, and H. Modares, ''Detection and mitigation of data manipulation attacks in AC microgrids,'' *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2588–2603, May 2020.

[145] S. Gholami, S. Saha, and M. Aldeen, ''A cyber attack resilient control for distributed energy resources,'' in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. Eur. (ISGT-Europe)*, Sep. 2017, pp. 1–6.

[146] V. K. Singh and M. Govindarasu, ''A cyber-physical anomaly detection for wide-area protection using machine learning,'' *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3514–3526, Jul. 2021.

[147] A. Patel, S. Roy, and S. Baldi, ''Wide-area damping control resilience towards cyber-attacks: A dynamic loop approach,'' *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3438–3447, Jul. 2021.

[148] M. Adeli, M. Hajatipour, M. J. Yazdanpanah, H. Hashemi-Dezaki, and M. Shafieirad, ''Optimized cyber-attack detection method of power systems using sliding mode observer,'' *Electric Power Syst. Res.*, vol. 205, Apr. 2022, Art. no. 107745.

[149] M. Zanetti, E. Jamhour, M. Pellenz, M. Penna, V. Zambenedetti, and I. Chueiri, ''A tunable fraud detection system for advanced metering infrastructure using short-lived patterns,'' *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 830–840, Jan. 2019.

[150] Z. Feng, J. Huang, W. H. Tang, and M. Shahidehpour, ''Data mining for abnormal power consumption pattern detection based on local matrix reconstruction,'' *Int. J. Electr. Power Energy Syst.*, vol. 123, Dec. 2020, Art. no. 106315.

[151] C. Sun, R. Zhu, and C. Liu, ''Cyber attack and defense for smart inverters in a distribution system,'' CIGRE Study Committee D2 Colloquium, Helsinki, Finland, Tech. Rep. NSF-PAR ID:10099566, 2019.

[152] P. Zhuang and H. Liang, ''False data injection attacks against state-of-charge estimation of battery energy storage systems in smart distribution networks,'' *IEEE Trans. Smart Grid*, vol. 12, no. 3, pp. 2566–2577, May 2021.

[153] D. Jafarigiv, K. Sheshyekani, M. Kassouf, Y. Seyedi, H. Karimi, and J. Mahseredjian, ''Countering FDI attacks on DERs coordinated control system using FMI-compatible cosimulation,'' *IEEE Trans. Smart Grid*, vol. 12, no. 2, pp. 1640–1650, Mar. 2021.

[154] S. M. Mohiuddin and J. Qi, ''Attack resilient distributed control for AC microgrids with distributed robust state estimation,'' in *Proc. IEEE Texas Power Energy Conf. (TPEC)*, Feb. 2021, pp. 1–6.

[155] Y. Chen, D. Qi, H. Dong, C. Li, Z. Li, and J. Zhang, ''A FDI attack-resilient distributed secondary control strategy for islanded microgrids,'' *IEEE Trans. Smart Grid*, vol. 12, no. 3, pp. 1929–1938, May 2021.

[156] A. Afshari, M. Karrari, H. R. Baghaee, and G. B. Gharehpetian, ''Resilient synchronization of voltage/frequency in AC microgrids under deception attacks,'' *IEEE Syst. J.*, vol. 15, no. 2, pp. 2125–2136, Jun. 2021.

[157] A. Y. Fard, M. B. Shadmand, and S. K. Mazumder, ''Holistic multi-timescale attack resilient control framework for power electronics dominated grid,'' in *Proc. Resilience Week (RWS)*, Oct. 2020, pp. 167–173.

[158] Z. Lian, F. Guo, C. Wen, C. Deng, and P. Lin, ''Distributed resilient optimal current sharing control for an islanded DC microgrid under DoS attacks,'' *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 4494–4505, Sep. 2021.

[159] S. Sahoo, Y. Yang, S. Member, and F. Blaabjerg, ''Resilient synchronization strategy for AC microgrids under cyber attacks,'' *IEEE Trans. Power Electron.*, vol. 36, no. 1, pp. 73–77, Jan. 2021.

[160] N. Duan, N. Yee, A. Otis, J.-Y. Joo, E. Stewart, A. Bayles, N. Spiers, and E. Cortez, ''Mitigation strategies against cyberattacks on distributed energy resources,'' in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2021, pp. 1–5.

[161] S. Peyghami, P. Davari, M. Fotuhi-Firuzabad, and F. Blaabjerg, ''Standard test systems for modern power system analysis: An overview,'' *IEEE Ind. Electron. Mag.*, vol. 13, no. 4, pp. 86–105, Dec. 2019.

[162] D. Rebollal, M. Carpintero-Rentería, D. Santos-Martín, and M. Chinchilla, ''Microgrid and distributed energy resources standards and guidelines review: Grid connection and operation technical requirements,'' *Energies*, vol. 14, no. 3, p. 523, Jan. 2021.

[163] S. Sahoo, Y. Yang, S. Member, and F. Blaabjerg, ''Resilient synchronization strategy for AC microgrids under cyber attacks,'' *IEEE Trans. Power Electron.*, vol. 36, no. 1, pp. 73–77, Jan. 2021.

[164] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, ''A framework for modeling cyber-physical switching attacks in smart grid,'' *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 2, pp. 273–285, Dec. 2013.

[165] A. Suzuki, K. Masutomi, I. Ono, H. Ishii, and T. Onoda, ''CPS-sim: Co-simulation for cyber-physical systems with accurate time synchronization,'' *IFAC-PapersOnLine*, vol. 51, no. 23, pp. 70–75, 2018.

[166] C. Kleijn, ''Introduction to hardware-in-the-loop simulation,'' Controllab Products B.V., Controllab, Enschede, The Netherlands, Tech. Rep., 2014, pp. 1–15.

[167] A. Khan, M. Hosseinzadehtaher, M. B. Shadmand, D. Saleem, and H. Abu-Rub, ''Intrusion detection for cybersecurity of power electronics dominated grids: Inverters PQ set-points manipulation,'' in *Proc. IEEE CyberPELS (CyberPELS)*, Oct. 2020, pp. 1–8.

[168] K. P. Schneider, J. C. Fuller, and D. Chassin, ''Evaluating conservation voltage reduction: An application of GridLAB-D: An open source software package,'' in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2011, pp. 1–6.

[169] J. H. Chow and J. J. Sanchez-Gasca, *Power System Modeling, Computation, and Control*. Hoboken, NJ, USA: Wiley, 2020.

[170] M. S. Sadabadi, Q. Shafiee, and A. Karimi, ''Plug-and-play robust voltage control of DC microgrids,'' *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6886–6896, Nov. 2018.

[171] S. M. Mohseni-Bonab, A. Hajebrahimi, I. Kamwa, and A. Moeini, ''Transmission and distribution co-simulation: A review and propositions,'' *IET Gener., Transmiss. Distrib.*, vol. 14, no. 21, pp. 4631–4642, Nov. 2020.

[172] W. Chen, D. Ding, H. Dong, and G. Wei, ''Distributed resilient filtering for power systems subject to denial-of-service attacks,'' *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 8, pp. 1688–1697, Aug. 2019.

[173] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, ''A cyber-attack resilient distributed control strategy in islanded microgrids,'' *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 3690–3701, Sep. 2020.

[174] D. Xie, J. Li, and H. Gao, ''Comparison and analysis of simulation methods for TSN performance,'' *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 768, no. 5, Mar. 2020, Art. no. 052061.

[175] Typhoon HIL. (2021). *Typhoon HIL604 Brochure*. Accessed: Aug. 6, 2021. [Online]. Available: https://www.typhoon-hil.com/doc/products/Typhoon-HIL604-brochure.pdf

[176] T. Hossen, F. Sadeque, M. Gursoy, and B. Mirafzal, ''Self-secure inverters against malicious setpoints,'' in *Proc. IEEE Electr. Power Energy Conf. (EPEC)*, Nov. 2020, pp. 3–8.

[177] S. Sahoo and S. Mishra, ''An adaptive event-triggered communication-based distributed secondary control for DC microgrids,'' *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6674–6683, Nov. 2018.

[178] M. Chlela, D. Mascarella, G. Joós, and M. Kassouf, ''Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks,'' *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4702–4711, Sep. 2018.

[179] Y. Shen, L. Wang, J. P. Lau, and Z. Liu, ''A robust control architecture for mitigating sensor and actuator attacks on PV converter,'' in *Proc. IEEE PES GTD Grand Int. Conf. Expo. Asia (GTD Asia)*, Mar. 2019, pp. 970–975.

[180] A. H. Pasdar, S. Azadi, and R. Kazemi, ''A comparative study on the efficiency of compiled languages? And MATLAB/simulink for simulation of highly nonlinear? Automotive systems,'' *J. Appl. Comput. Mech.*, vol. 8, no. 3, pp. 1–12, 2021.

[181] B. Azimian, P. M. Adhikari, L. Vanfretti, and H. Hooshyar, ''Cross-platform comparison of standard power system components used in real time simulation,'' in *Proc. 7th Workshop Modeling Simulation Cyber-Phys. Energy Syst. (MSCPES)*, Apr. 2019, pp. 1–6.

[182] I. Grinberg, M. Meskin, and M. Safiuddin, "Test bed for a cyber-physical system (CPS) based on integration of advanced power laboratory and eXtensible messaging and presence protocol (XMPP)," in *Proc. ASEE Annu. Conf. Expo.*, 2015, p. 21451.

[183] Y. Xue and X. Yu, "Beyond smart grid—Cyber–physical–social system in energy future [point of view]," *Proc. IEEE*, vol. 105, no. 12, pp. 2290–2292, Dec. 2017.

[184] E. Vugrin, A. R. Castillo, and C. A. Silva-Monroy, "Resilience metrics for the electric power system: A performance-based approach," Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND2017-1493654236, 2017.

[185] B. Sahoo, S. K. Routray, and P. K. Rout, "AC, DC, and hybrid control strategies for smart microgrid application: A review," *Int. Trans. Electr. Energy Syst.*, vol. 31, no. 1, p. e12683, 2021.

[186] J. Eto, R. Lasseter, D. Klapp, A. Khalsa, B. Schenkman, M. Illindala, and S. Baktiono, "The certs microgrid concept, as demonstrated at the certs/aep microgrid test bed," Lawrence Berkeley Nat. Lab., Berkeley, CA, USA, Tech. Rep., Sep. 2018.

[187] X. Li, C. Chen, Q. Xu, and C. Wen, "Resilience for communication faults in reactive power sharing of microgrids," *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 2788–2799, Jul. 2021.

[188] N. D. Tuyen, L. V. Thinh, V. X. S. Huu, and G. Fujita, "Forecasting I–V characteristic of PV modules considering real operating conditions using numerical method and deep learning," in *Proc. Int. Conf. Smart Grids Energy Syst. (SGES)*, Nov. 2020, pp. 544–549.

NGUYEN DUC TUYEN received the bachelor's degree in electrical engineering from the Hanoi University of Science and Technology, in 2006, and the master's and Ph.D. degrees from the Shibaura Institute of Technology, Tokyo, Japan, in 2009 and 2012, respectively. From 2012 to 2015, he was a Researcher at the Shibaura Institute of Technology and a part-time Lecturer at Chiba University and Tokyo Wildlife College, Japan. From 2015 to 2017, he worked at the Tokyo University of Science, Tokyo. From 2017 to 2018, he conducted the research at the National Institute of Industrial Science and Technology, Japan. Since 2018, he has been a Lecturer of the Department of Electrical Engineering, School of Electrical and Electronic Engineering, Hanoi University of Science and Technology. He has published more than 120 journal and conference papers. He is an active reviewer of IEEE, IET, MDPI, IEEJ, Springer, and Elsevier and has been reviewing hundreds of papers, since 2009.

NGUYEN SY QUAN is currently an Electrical Engineering Student major in control engineering and power system at the Hanoi University of Science and Technology, where he is also a Research Assistant under the supervision of Dr. N. D. Tuyen at 100% Renewable Energy Laboratory. He has been working on several national projects with Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) and Vietnam Initiative for Energy Transition Social Enterprise (VIETSE). Regarding the research of smart grid cybersecurity, he is also working with VIETSE to initiate the research on data mining-based detection of FDIA and DoS in DC microgrid. His research interests include advanced control system in microgrid, cyberattack detection and mitigation in power systems, electricity market, BESS, and power electronics.

VO BA LINH is currently an Electrical Engineering Student major in control engineering and power system at the Hanoi University of Science and Technology. He is also part of the 100% Renewable Energy Research Team in his university and a Technical Intern of GIZ, which mainly concerns supporting national policy planning. He is a frequent attendee of academic events in his university and around the world. He has published the first paper in Student Forum 2020 as part of Vietnam–Germany Cooperation Program. His research interests include advanced control system in microgrid, cyberattack detection, and mitigation in power system with distributed power sources.

VU VAN TUYEN (Member, IEEE) received the B.S. degree in electrical engineering from the Hanoi University of Science Technology, Vietnam, and the Ph.D. degree in electrical engineering from Florida State University, in 2016. From 2016 to 2017, he was a Postdoctoral Research Associate at the Center for Advanced Power Systems, Florida State University, where he was a Research Faculty, from 2017 to 2018. Since July 2018, he has been an Assistant Professor at Clarkson University, NY, USA. His research interests include smart grid; power system dynamics, stability, and control; energy management and optimization; and power systems cybersecurity and integration of DERs into power systems. He has published over 50 technical conference and journal papers, in which one received the 2021 Best Paper Award of the *IEEE Industrial Electronics Magazine*. He has also organized, chaired, and cochaired IEEE conferences such as IEEE IECON and IEEE ESTS conferences. He has been a Guest Editor of IEEE Transactions on Industrial Informatics, in February 2020, for the Special Issue on Resilience, Reliability, and Security in Cyber-Physical Systems.

GORO FUJITA (Member, IEEE) received the B.E., M.E., and Ph.D. degrees in electrical engineering from Hosei University, Tokyo, Japan, in 1992, 1994, and 1997, respectively. He is currently a Professor at the Shibaura Institute of Technology, Tokyo. His research interest includes power system control. He is a member of the IEE of Japan.