Cybersecurity in Virtual Power Plants: A Review of Theoretical Framework, Risk Analysis, and Defense Technologies

Jiayu Li, Hongchao Gao, *Member*, *IEEE*, Chongqing Kang, *Fellow*, *IEEE*, Yiwei Cui, Wenmeng Zhao, and Tian Mao

***Abstract*—Virtual power plants (VPPs) can participate in electricity market trading by aggregating distributed energy resources, thereby providing flexible regulation services to the power system. However, the interaction between VPPs and the power system involves high-frequency and multi-party data exchange, posing significant cybersecurity risks. To ensure the cybersecurity of VPPs throughout the entire interaction process, this paper first analyzes the intrinsic attributes of VPPs, identifying three key characteristics: aggregation, interaction, and regulation. Based on this, it integrates these attributes with confidentiality, integrity, and availability triad to construct a cybersecurity theoretical framework for VPPs. Second, this paper outlines the business processes, data interactions, and communication architecture of VPPs. Then, a risk analysis of potential cyberattacks is performed, detailing their injection points, propagation paths, and potential impacts of typical cyberattacks. Third, the core application mechanisms and use cases of key cybersecurity defense technologies are summarized. These technologies are applicable to interactions between VPP and power systems across different stages, including data anonymization, encryption, privacy-preserving computation, access control, and blockchain. Finally, an analysis of the current status, challenges, and prospects of artificial intelligence (AI)-based cybersecurity technologies is presented, which provides support for constructing a secure and reliable cybersecurity defense system for VPPs.**

***Index Terms*—Virtual power plant (VPP), electricity market, artificial intelligence (AI), cyberattack, cybersecurity, risk, privacy-preserving computation, defense.**

I. Introduction

THE pursuit of "carbon peaking and carbon neutrality" goals has precipitated profound structural shifts in the energy supply and demand of power system. On the supply side, the installed capacity of renewable energy has surpassed that of thermal power [1], significantly intensifying the challenge of supply-demand balancing. On the demand side, rising end-use electrification has escalated the need for interaction between demand-side users and the power system; however, mechanisms to effectively mobilize the flexible regulation potential of these resources remain insufficient.

Against this backdrop, VPPs have emerged as a pivotal solution to the structural shortage of flexible regulation resources. By aggregating distributed energy resources, VPPs respond to multi-timescale regulation demands across different power system operators (e.g., transmission and distribution). Ever since the VPP concept is proposed, given the significant heterogeneity and high output uncertainty of aggregated resources, extensive research has focused on key technologies, specifically aggregation and regulation, to ensure the secure and efficient interaction between VPP and power system. For instance, [2] reviews the mainstream aggregation algorithms including vertex and half-plane methods based on Minkowski sums. Reference [3] utilizes statistical analysis of literature from 2013 to 2024, identifies key research hotspots, and highlights future directions such as high-dimensional uncertainty modeling and multi-timescale scheduling optimization. Reference [4] focuses on the operational characteristics and trusted quantification of distributed energy resources, summarizing challenges in the modeling of external characteristics and construction of optimal resource portfolio.

While these studies contribute significantly to the efficient interaction between VPP and power system, VPPs face challenges across two distinct dimensions. The first is physical security, involving system stability risks caused by resource output fluctuations and shifts in user's behavior. The second is cybersecurity, encompassing risks to communication, data, and privacy arising from cyberattacks. For VPPs, a successful cyberattack not only invalidates regulation responses to grid dispatch commands, which directly destabilize the supply-demand balance of power system, but also exposes aggregators to severe economic losses or contractual penalties.

Manuscript received: January 12, 2026; revised: April 17, 2026; accepted: June 1, 2026. Date of CrossCheck: June 1, 2026. Date of online publication: June 19, 2026.

This work was supported by the Smart Grid-National Science and Technology Major Project (No. 2025ZD0804500).

J. Li, H. Gao (corresponding author), and C. Kang are with Department of Electrical Engineering, Tsinghua University, Beijing 100084, China (e-mail: lijiayu1996@mail.tsinghua.edu.cn; hcgaoth@mail.tsinghua.edu.cn; cqkang@mail.tsinghua.edu.cn).

Y. Cui is with KTH Royal Institute of Technology, Stockholm, Sweden (e-mail: yiwei.cui0812@gmail.com).

W. Zhao and T. Mao are with Electric Power Research Institute, China Southern Power Grid, Guangzhou 510663, China (e-mail: zhaowm@csg.cn; tianmao7658@126.com).

DOI: 10.35833/MPCE.2026.000042

Furthermore, simultaneous attacks on multiple large-scale VPP aggregators can trigger cascading effects, leading to widespread failure of dispatching instructions or even massive equipment disconnection from the grid. These cross-domain penetration risks have already manifested in real-world scenarios. For instance, the Ukraine power grid attack in 2015 demonstrated how seizing control of dispatching systems could lead to large-scale blackouts. Similarly, the ransomware attack on Brazil's Light S.A. in 2020 encrypted internal files and paralyzed billing and service systems, disrupting commercial operations and severely compromising the secure and stable operation of power system [5].

In response to these emerging threats, existing literature addresses VPP technologies and cybersecurity from three primary streams. The first stream of research focuses on the development trends, technical frameworks, and core operational models of VPPs. Within this body of research, while many papers acknowledge the communication risks and cybersecurity issues associated with VPPs, they often treat them as a secondary concern. For example, [6] notes that the development of the smart grid increases cybersecurity and data privacy risks in the power system to some extent; however, the central focus of [6] investigates trading models for VPP participation in electricity markets and applicable scenarios for different optimization models. Similarly, although [7] and [8] identify user privacy protection as a mandatory requirement across the entire data chain, they focus on discussing the series of challenges faced in VPP operations from a "cyber-physical-social" perspective.

The second stream investigates specific privacy-preserving technologies, but lacks a systemic framework. For instance, while [9] mentions the importance of user privacy protection, its core research focuses on constructing a market trading framework using blockchain technology to protect the identities of the trading parties. Similarly, although [10] and [11] highlight the issue of privacy protection, they focus on achieving the optimal economic dispatch for VPPs under cybersecurity constraints, rather than systematically constructing a privacy protection framework.

The third stream examines the general cybersecurity of power system, but fails to conduct an in-depth analysis that incorporates the unique characteristics of VPPs, specifically the aggregation of massive heterogeneous resources and high-frequency interactions with power system. For example, [12] systematically reviews the privacy attacks and corresponding cybersecurity protection strategies in smart grids, but lacks a specific context for VPP scenarios. References [13] and [14] provide an in-depth analysis of the application of homomorphic encryption (HE) in VPPs, achieving user's privacy protection while ensuring the data validity. Nonetheless, they primarily concentrate on the single-stage resource aggregation of VPPs, while the complex and multi-party interactions among the VPPs, power system, and end-users are largely unaddressed.

In summary, existing literature has covered the majority of key areas in cybersecurity in VPPs, including technical system classifications, point-to-point privacy protection, and general cybersecurity reviews. Despite these contributions, current research lacks a comprehensive framework that aligns cybersecurity measures with the intrinsic attributes of VPPs. Specifically, as an emerging organizational model for power operation, VPPs possess core attributes, namely aggregation, interaction, and regulation (AIR), which distinguish them from traditional power system entities. The multi-party interactions between VPP and power system revolve around these three core attributes, giving rise to endogenous security vulnerabilities and domain-specific risks distinct from those of traditional power systems. Consequently, research on the cybersecurity in VPPs cannot simply replicate established findings from power system studies. Instead, it should be based on an analysis of the unique cybersecurity challenges VPPs face compared with traditional power systems, providing a systematic discussion on potential cyberattack vectors and their impacts, corresponding to the key cybersecurity defense technologies including their strengths, weaknesses, application scenarios, and key future trends.

Based on the aforementioned discussion and addressing the systemic gaps in current research on the cybersecurity in VPPs, the main contributions of this paper can be summarized as follows.

1) It establishes a cybersecurity theoretical framework for VPPs, which analyzes their intrinsic attributes, business processes, and cybersecurity requirements for the communication architecture of VPPs in the interactions with power system.

2) It conducts a risk analysis of potential cyberattacks against VPPs and their impacts, detailing the injection points, propagation paths, and potential consequences.

3) It summarizes the key cybersecurity defense technologies for VPPs across different business stages, and discusses the challenges and future trends.

The remainder of this paper is organized as follows. Section II presents the cybersecurity theoretical framework for VPPs. Section III presents the risk analysis of potential cyberattacks against VPPs and their impact analysis. Section IV presents the key cybersecurity defense technologies for VPPs. Section V presents the conclusion and outlook of this paper.

II. Cybersecurity Theoretical Framework for VPPs

A. Analysis of Intrinsic Attributes of VPPs

To construct a cybersecurity theoretical framework for VPPs, it is necessary to first analyze and refine the intrinsic attributes of VPPs to identify their intrinsic attributes, thereby distinguishing them from other market entities [15]. Firstly, the physical essence of a VPP must address what is meant by "virtual" and what constitutes the "power output". The term "virtual" emphasizes its non-physical form and signifies its characteristic of virtual power output. The term "power plant" suggests its operational behavior after aggregation and defines the operational scope of its business. A VPP is not a physical power plant; its physical entities are the demand-side resources. Therefore, a VPP itself is a special type of resource that does not have an independent physical existence. While management platforms empower VPP aggregation, they function fundamentally as technical enablers rather than the underlying physical resources. It is es-

sentially a technical support platform rather than the resource itself. The key concept in this process is "aggregation": the effective aggregation of the regulation capabilities of massive distributed energy resources, which are then represented as an independent, power plant-like market entity from the perspective of power system operator and electricity markets.

Secondly, the technical principle of a VPP stems from its original intent: to unlock the flexibility of demand-side resources. From the perspective of supply-demand balance in the power system, a reduction in electricity consumption at a given time is equivalent to an increase in generation. The VPP must provide a virtual response of "power plant" for balancing both energy and power in multi-timescales. The recognition of its virtual output is established through its interactive regulation with the power system. The key concept in this process is "interaction", which refers to achieving interaction between massive distributed energy resources and the power system through the VPP as a special entity. Regarding the core attribute of "interaction", it is essential to clarify that although many scholars consider demand response (DR) and VPPs to have significantly overlapping participants, intersecting scenarios, and similar service capabilities, conceptual differences persist from an interaction perspective. In terms of core objectives, DR is a market-driven optimization tool for demand-side consumption behavior centered on flexible load regulation. Conversely, a VPP serves as an equivalent controllable power source comparable to traditional power plants, providing the power system with multi-timescale bidirectional balance support for both energy and power. Regarding role positioning, DR primarily facilitates minute-to-hour scale unidirectional or quasi-bidirectional slow dynamic adjustments (particularly in China where DR is viewed as a relatively narrow service mechanism, i.e., a service entity for supply-demand balance in scenarios with insufficient system regulation capacity). In contrast, VPPs operate as independent market entities that can compete alongside traditional generating units, with regulation capabilities spanning all system balancing requirements from frequency regulation to peak-shaving and valley-filling.

Finally, the core resource of a VPP is its dispatchable load. If the load resources do not have regulation capability, the "output" of VPP will cease to exist, and it cannot function as a "power plant" that can be dispatched by the power system. The key concept in this process is "regulation", by leveraging the dispatchable capability of demand-side resources to achieve upward or downward power adjustments based on power system dispatching commands. In summary, only by satisfying the three key characteristics of AIR can a VPP be routinely dispatched by the power system as a conventional power plant resource.

Based on the three intrinsic attributes identified above, i.e., AIR, it is evident that fundamental differences exist between VPPs and various market entities in traditional power systems. These distinctions render the cybersecurity analysis theories and frameworks of conventional power system inadequate for being directly applied to address challenges in the cybersecurity in VPPs. To address this gap, this paper synthesizes the widely recognized confidentiality, integrity, and availability (CIA) triad with AIR to conduct a comprehensive analysis. The endogenous drivers, core requirements, and unique characteristics of VPP cybersecurity relative to traditional power systems will be detailed in the following text.

From the aggregation perspective, significant differences exist between VPPs and traditional power systems regarding their attack surfaces. Specifically, large generating units in traditional power systems operate with well-defined parameters and stringent cybersecurity protocols, typically deployed within dedicated networks. In contrast, a VPP needs to effectively aggregate the regulation capabilities of massive demand-side resources. However, these resources have diverse characteristics and are geographically dispersed. A thorough understanding of their generation/consumption patterns and regulation potential is required to dispatch them according to the dispatching commands from power system operator. Drawing upon widely adopted cybersecurity principles for power and industrial control systems, including network segmentation, dedicated operational networks, zone isolation, and authenticated inter-system communications, demand-side resource devices are typically located in the secure access perimeter of the cybersecurity architecture of power system. However, given that these massive distributed devices originate from diverse manufacturers and vary in models, it proves to be difficult to enforce unified cybersecurity standards and ensure comprehensive, timely updates. VPPs are unable to implement unified full-lifecycle cybersecurity management for such massive and decentralized terminal devices. Consequently, some devices may rely on outdated cybersecurity measures or lack essential vertical encryption and identity authentication mechanisms. The process of VPPs aggregating distributed energy resources and participating in market trading introduces both aggregators and demand-side resources, involving the transmission and interaction of massive amounts of data. This necessitates research into areas such as trusted authentication, access control, and privacy protection for user data to prevent the unauthorized access of sensitive user's data.

From the interaction perspective, upon aggregating massive heterogeneous distributed energy resources, the VPP functions as a unified entity to interact with the power system. For the operation of traditional power system, a unidirectional regulation paradigm of "generation-following-load" is typically adopted, where critical information and dispatching commands are predominantly issued by the power system to individual large-scale generating units. In contrast, VPP business processes span the entire lifecycle, including resource aggregation, transaction declaration, market clearing, dispatching execution, and information disclosure, involving high-frequency and bidirectional interactions among multiple entities such as power dispatching agencies, power exchange centers, VPP aggregators, and distributed energy resource owners. This open interaction model across different entities and cybersecurity partitions, characterized by dynamically changing interaction participants, links, and data types, renders each cross-entity and cross-partition data exchange a potential vector for cyberattack penetration and

cross-domain propagation. Consequently, safeguarding the integrity and availability of bidirectional transmission is paramount to mitigating potential cyberattacks and limit their propagation. This protection mechanism ensures that operational data remain authentic and tamper-proof during interactions with the power system.

From the regulation perspective, within the context of traditional power system operations, significant impacts generally require an attacker to breach and compromise either the grid dispatch system or the control systems of large-scale generation units. However, the precise response of VPPs to grid dispatch commands follows a logical operational chain consisting of dispatch command reception, decomposition of multi-resource command, terminal collaborative execution, operational status feedback, and adjustment of dynamic regulation strategy. Throughout this process, it is essential to safeguard the authenticity and consistency of both dispatching and execution commands. This operational logic implies that an attacker only needs to gain control over a specific scale of terminal devices of distributed energy resources to mislead the global regulation decisions of the VPP aggregation platform. By forging terminal operational statuses or tampering with execution feedback data, they can induce the platform to issue incorrect dispatch commands, thereby threatening the supply-demand balance and stable operation of power system. Therefore, this necessitates the precise identification, decomposition, and dissemination of instructions while simultaneously defending against malicious activities such as command forgery and feedback spoofing. By securing the entire execution chain, VPPs guarantee the availability and reliability of information, ultimately enabling precise regulation in response to the dispatching commands from power system operator.

B. Business Process of VPPs in Interactions with Power System

Similar to other market entities, VPPs must adhere to unified rules when participating in electricity trading. Its business process can generally be divided into five key stages: resource aggregation, transaction declaration, market clearing, dispatching execution, and information disclosure [16]. Among these, the resource aggregation stage is a necessary and unique step for VPPs compared with other market entities before they obtain the qualification for accessing the power system. Information exchange in this stage is at low frequency, typically triggered only by updates to user registration profiles such as changes in corporate details, substantial alterations to resource composition (e.g., quantity or category), or adjustments to market business scopes, and the type of market transaction-related business. Specifically, the process begins with the VPP aggregator and distributed energy resources signing business contracts on aggregation system or platform. Subsequently, the power system operator conducts tests to access the power system and obtain the certification for the VPP aggregated resources. The certification evaluates capabilities across three core dimensions: regulation performance (including dispatchable capacity, regulation rate, and deviation), communication quality (covering data accuracy, latency, and transmission reliability), and cybersecurity (focusing on encryption standards and cybersecurity protection protocols) [17].

In the transaction declaration stage, upon successfully passing basic functional tests for accessing the power system, the VPP submits its quantity-price curve to the power exchange center during the day-ahead market bidding phase [18]. Information exchange in this stage primarily occurs on a day-ahead basis, supplemented by intra-day rolling adjustments. Once the unit and power system operational parameters issued by the power system operator such as day-ahead load forecasts, transmission equipment maintenance schedules, key network section constraints, and must-run/must-stop units are confirmed, the VPP aggregator follows the standard market participation workflow to formulate and submit a quantity-price bidding curve in the day-ahead timeframe. This strategy is developed by considering the generation and consumption status of its resources, historical trading data, and other influencing factors such as the regulation capability, operational costs, and regulation willingness of aggregated resources, with the objective of maximizing economic benefits [19], [20].

The market clearing stage primarily involves information interaction between the power system operator and the power exchange center. In this stage, the power system operator utilizes the quantity-price bidding curves submitted by market entities including VPP aggregators. These curves represent the aggregated technical constraints and economic offers of the VPP, which are treated by the power exchange center as coming from a single VPP with defined hourly outputs [21]. Based on predictions of the supply-demand balance constraints of power system and the operating boundary constraints of market participants, the power system operator solves the security-constrained unit commitment (SCUC) and security-constrained economic dispatch (SCED) calculations sequentially. This process determines the winning unit commitment, generation curves, and time-differentiated prices for market entities on the actual operating day. This stage involves large-scale and high-precision calculations with massive amounts of data, making it computationally demanding, and is typically performed in the cloud platform [22]. Additionally, in the intra-day stage, the power system operator needs to adjust the operating plan based on changes in system operating conditions to correct for deviations between day-ahead schedule and real-time operation.

The dispatching execution stage takes place on the actual operating day. The VPP aggregator formulates the power schedule for its aggregated resources based on the market clearing results issued by the power exchange center. Subsequently, it decomposes and issues corresponding dispatching commands via communication links to local control systems or intelligent terminal devices, driving the resources to adjust output or execute start-stop operations at specified timestamps. Throughout this process, the VPP aggregator needs to frequently collect generation and consumption data from the distributed energy resources, and then report, verify, and provide feedback in real time to ensure a precise response to the dispatching commands from power system operator [23].

The information disclosure is primarily the responsibility of the power exchange center. After the actual operating day, it must accurately, promptly, and completely release information to the market entities as required by power system operator. This includes public information (e.g., the market-wide nodal weighted average price for each trading period), private information for generation units, and VPP aggregators (e.g., the unit on/off status for the 96 intervals of the operating day, the hourly awarded energy, and the corresponding hourly average nodal price) [24]. Figure 1 summarizes the business process for VPPs in interactions with power system and market operations.

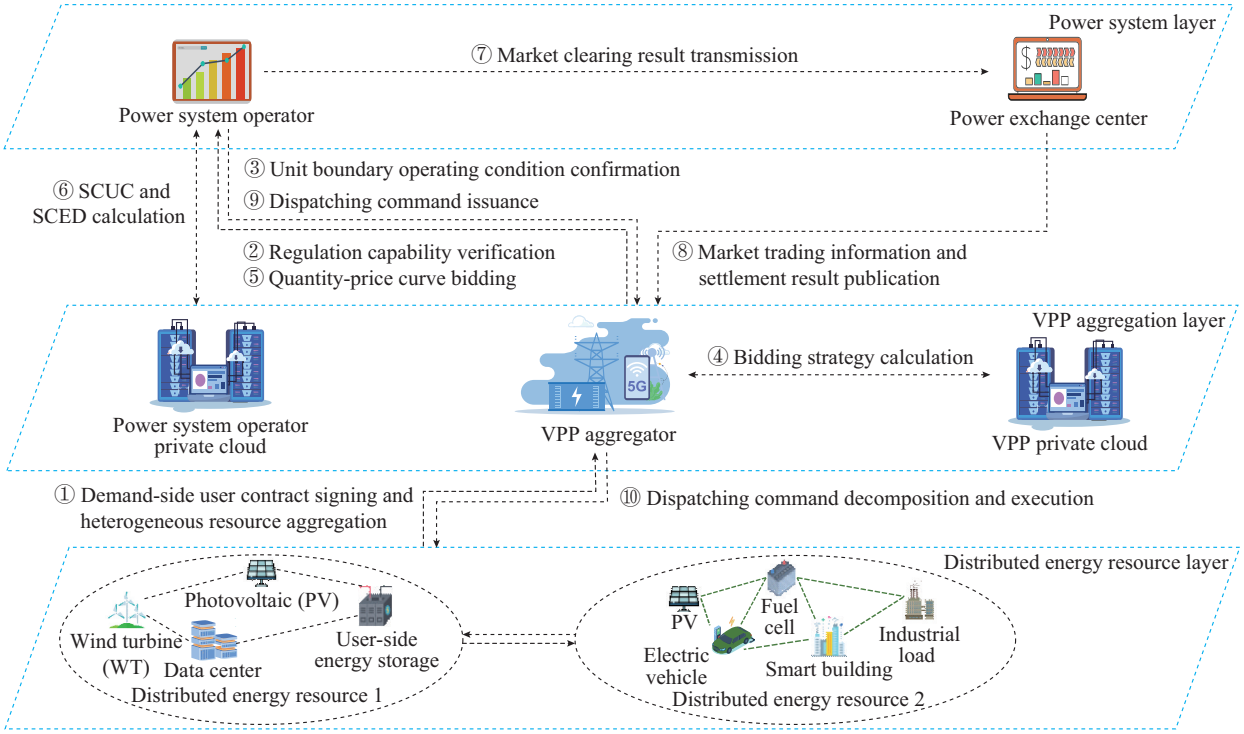

Fig. 1. Business process for VPPs in interactions with power system and market operations.

Table I summarizes the typical data interactions and corresponding frequencies of VPPs in the interactions with power system. To facilitate a clearer discussion of the impacts of different cyberattacks, this paper categorizes the data in Table I into four main types: directly acquired data (i.e., data collected directly from terminal devices), dispatching data (i.e., data related to the execution of dispatching commands among demand-side users, VPP aggregators, and power system operator), trading data (i. e., market trading data involved in stages such as bidding and clearing between the VPP aggregator and the power exchange center), and management data (i.e., data related to the management of user's information by VPP aggregator). Analysis of the data in Table I reveals that the interaction of VPP with the power system embodies the core concepts of AIR, and nearly all stages involve massive data interaction. Apart from management data, which is updated less frequently, the update and interaction frequencies for directly acquired, dispatching, and trading data are typically at the second-to-minute level in actual market operations. This imposes relatively high real-time requirements on data interaction.

TABLE I
TYPICAL DATA INTERACTIONS AND CORRESPONDING FREQUENCIES OF VPPS IN INTERACTIONS WITH POWER SYSTEM

Key stage	Specific process included	Key data involved	Entity involved	Interaction frequency
Resource aggregation	Demand-side contract signing, capacity aggregation, and capability verification	User's information, device information, historical generation and consumption data, and regulation range and rate	Demand-side user, VPP aggregator, and power system operator	Monthly/upon update
Transaction declaration	Market boundary confirmation and bidding strategy formulation	Unit constraints, maintenance schedules, and VPP quantity-price bidding curves	VPP aggregator and power exchange center	Daily to hourly
Market clearing	SCUC and SCED calculation and result publication	Cleared power curves, nodal prices, and network section constraints	Power system operator, power exchange center, and VPP	15 min to 1 hour
Dispatch execution	Command decomposition, terminal execution, and real-time feedback	Decomposed output curves, real-time device status, and regulation deviation	VPP aggregator and demand-side user	Seconds to 15 min
Information disclosure	Post-operation data release and settlement result publication	Market-wide nodal prices, hourly awarded energy, and on/off status of generation unit	Power exchange center and market entities	Daily, post-operation

C. Cybersecurity Requirements for Communication Architecture of VPPs

To support the complex business-level interactions between VPPs and the power system, the communication architecture of VPPs must be highly coordinated in function and strictly compliant with the cybersecurity standards. To systematically analyze these requirements, this paper adopts an architecture-based analysis method [25], which examines the information transmission chain across the four-layer functional hierarchy (cloud-tube-edge-terminal) of the VPPs.

The terminal layer is primarily composed of massive, heterogeneous, and geographically dispersed distributed energy resources (e. g., PV inverters and energy storage), controllable loads (e. g., smart air conditioners and electric vehicle chargers), and metering devices (e. g., smart meters). These massive terminal devices, through built-in sensors and controllers, generate key operational data in real time such as telemetry data (e. g., voltage, current, power, and state of charge of battery) and switch status signals. The data are first preliminarily processed by the control unit within the device and are then collected by the edge layer. The core cybersecurity requirement on the terminal layer is to ensure the authenticity of device identities and the reliability of data sources, preventing physical tampering and device spoofing attacks [26].

The edge layer, acting as a critical hub connecting the terminal layer and cloud layer, is typically composed of hardware entities deployed in proximity to resource sites (e.g., industrial parks or commercial building clusters) to serve as local data processing and proxy nodes. The core function of the edge layer is to solve the challenge of providing unified access and data standardization for massive, underlying heterogeneous resources, while also supporting the rapid local processing of some lightweight decision-making tasks. To achieve broad device connectivity, the edge computing gateway with its diverse physical interfaces can connect to centralized and site-based resources via industrial Ethernet, serial communication (e.g., RS-485), or field buses (e.g., controller-area network bus). It can also use wireless networks such as 5G and LoRa to cover dispersed and small-scale resources. Before uploading data, given that terminal devices use various protocols, the edge computing gateway needs to perform unified data conversion. By deeply parsing multiple communication protocols such as Modbus, IEC 61850, and message queuing telemetry transport (MQTT) [27], [28], it decodes the collected raw data frames and encapsulates them into a unified, structured data format, thereby creating a standardized information flow. Additionally, the edge computing gateway can also perform local tasks such as data cleaning and outlier filtering. On the actual operating day, it precisely executes the decomposed dispatching commands from the VPP aggregator. All externally transmitted data are encrypted at the edge intelligence gateway, and transmitted using secure communication technologies such as virtual private networks (VPNs) to ensure the CIA of data [29].

The tube layer, as the core channel between the edge and the cloud, is typically divided into two types of networks based on cybersecurity levels and business attributes. The dedicated power network primarily carries production or control data that have extremely high cybersecurity and real-time requirements. Real-time data from the edge computing gateway such as telemetry, remote signaling, remote control, and remote regulation are processed by a power vertical encryption and authentication device. They are then transmitted to the cloud platform via highly reliable dedicated lines such as optical fiber. The public power network is used for non-control business, carrying management information with lower real-time requirements such as user resource and billing data in smart meters. The data can be transmitted over public communication networks such as 5G, and sent to the management information zone of the cloud platform after being encrypted via a VPN. Cybersecurity devices such as intrusion detection systems and network boundary firewalls are typically deployed at the public network boundary to block and identify the penetration attacks [30].

The cloud layer is the central hub where the VPP and power system operator execute complex global decision-making and optimization. According to the secondary cybersecurity protection principles of power system [31], application systems (e.g., energy management system (EMS) and office automation system oriented toward power system enterprises and large-scale power generation enterprises) with different cybersecurity levels on the cloud platform are strictly divided into different cybersecurity zones. Physical isolation is typically enforced between zones, while logical isolation based on technologies such as firewalls and access control is used within a zone. The specific division of these zones is as follows.

1) Production control zone. This is the core control zone for the secure operation of VPP and power system with the highest security level. For example, in the actual deployment and application of power system in China, it is further subdivided into Zone I (real-time control area) and Zone II (non-control production area). It receives real-time data streams from the edge layer via the dedicated network. Typical systems deployed in this zone include the EMS, supervisory control and data acquisition (SCADA) system, and real-time control systems. These systems are primarily responsible for real-time monitoring, operational control, and statistical analysis of energy generation and consumption for various market entities. A cyberattack on this zone would directly threaten the physical security of the power system [32].

2) Management information zone. Comprising Zone III (production management area) and Zone IV (management information area) of the power system in China, this zone primarily receives non-real-time data from the production control zone or directly receives management data from the public network. Typical systems deployed here include the VPP aggregation system, billing and settlement system, and office automation system. These systems handle business functions such as market bidding, electricity bill calculation, and operation and maintenance management, which are not involved in the direct control of the power system.

In the aforementioned four-layer functional hierarchy (cloud-tube-edge-terminal), each step of the VPP information flow corresponds to specific devices, interfaces, and protocols.

This layered and zoned architecture provides a foundation for the precise analysis of the injection points, propagation paths, and potential risks of different types of cyberattacks.

D. Analysis of Endogenous Drivers for Cybersecurity Risks

The analysis of cybersecurity issues in VPPs can be based on the internationally recognized CIA triad. This triad consists of three principles: ① confidentiality, which restricts information access, ensuring that data can only be accessed by authorized users or systems; ② integrity, which focuses on ensuring the completeness and authenticity of information during transmission; and ③ availability, which ensures that authorized users have timely and reliable access to system resources. Implementing this framework is essential yet challenging due to the inherent complexity and uncertainty of VPP functional modules, which face evolving cybersecurity risks [33]. Once a cyberattack on a VPP succeeds, it will impact the intrinsic attributes and operational workflows of VPPs to varying degrees, depending on which element of the CIA triad the attacker targets.

Confidentiality violations manifest primarily as data leakage. Regarding aggregation, the leakage of demand-side generation and consumption data as well as device parameters can significantly reduce user's willingness to participate in the aggregation programs. Regarding interaction, the compromise of sensitive information such as VPP market bidding strategies, quantity-price curves, and commercial operational data causes the VPP to lose its competitive edge in electricity markets and may even lead to its involuntary involvement in market manipulation. Regarding regulation, the leakage of core dispatch data, including regulation plans and reserve capacities provides attackers with the intelligence needed to accurately predict system states and launch subsequent targeted strikes, directly threatening the security of power system dispatch.

Integrity violations primarily manifest as data tampering and command forgery. Regarding aggregation, the tampering of fundamental data such as the regulation capacity, operational status, and rated capacity of distributed energy resources leads to inaccurate assessments of the aggregation capability of VPP, hindering the effective utilization of heterogeneous resources. Regarding interaction, the alteration of core information such as market clearing results, settlement data, and cross-entity interaction commands can result in transaction defaults, disrupting normal market order. Regarding regulation, the tampering of critical data including dispatch commands, terminal execution feedback, and regulation deviation data causes VPP responses to deviate from power system requirements, directly threatening the stable operation of power system.

Availability violations manifest as service interruptions and link failures. Regarding aggregation, interruptions in terminal data collection channels or edge gateways prevent the VPP from acquiring real-time resource status, leading to a loss of control over massive aggregated resources. Regarding interaction, outages in market trading platforms or cross-entity communication links prevent the VPP from completing bidding declarations and information exchanges, disabling its core market participation functions. Regarding regulation, the paralysis of dispatch command channels or terminal control systems renders the VPP unresponsive to grid dispatch commands, detrimentally impacting the supply-demand balance and overall security of power system.

Based on the comprehensive synthesis of the intrinsic attributes of VPP (i.e., AIR) and the systematic analysis of how violations of the CIA principles impair these functionalities, Fig. 2 illustrates the interaction relationship between the intrinsic attributes of VPPs and the three principles of cybersecurity. This mapping serves as a solid theoretical foundation to help visualize how specific cyber threats propagate across different operational domains and to identify corresponding defense priorities.

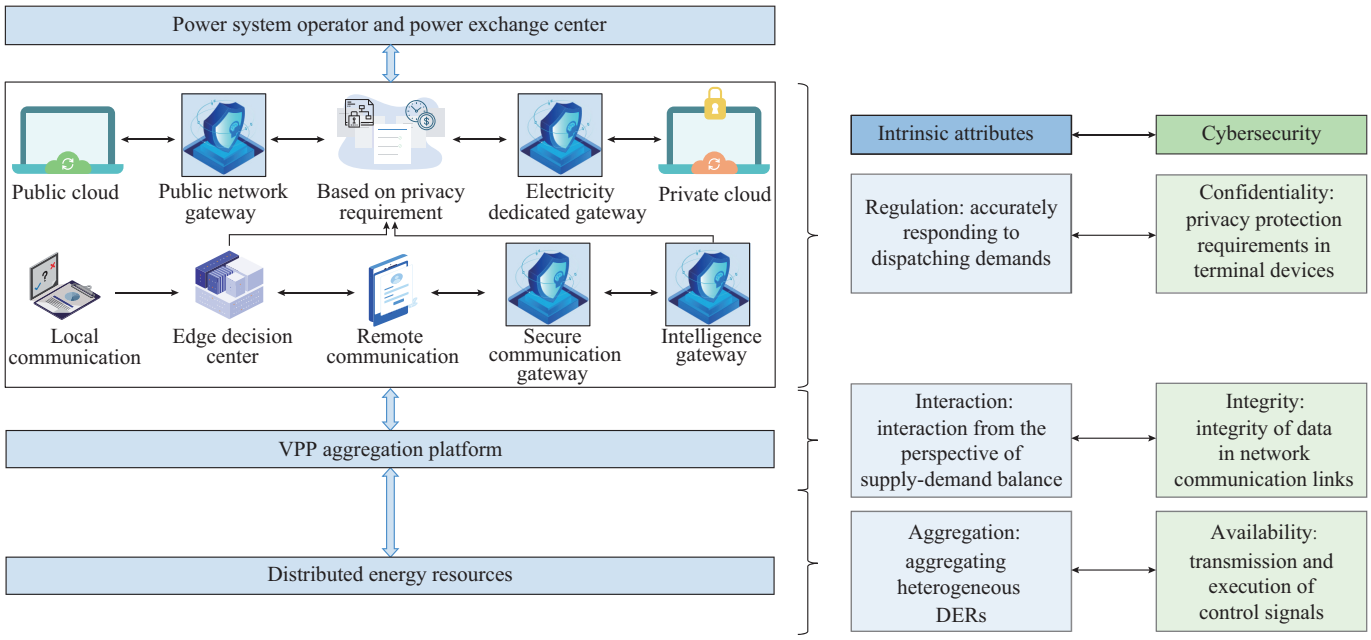

Fig. 2. Schematic diagram of interaction relationship between intrinsic attributes of VPPs and three principles of cybersecurity.

III. Risk Analysis of Potential Cyberattacks Against VPPs and Their Impact Analysis

A. Potential Cyberattacks in VPPs

In practice, existing cyberattacks are numerous, complex, and constantly evolving. According to statistics from the Common Attack Pattern Enumeration and Classification database maintained by the U.S. Department of Homeland Security, the number of derived cyberattack patterns globally has exceeded 2000. Therefore, it is nearly impossible to conduct a detailed analysis of all current cyberattack methods. To address this challenge, this paper categorizes potential cyberattacks in VPPs based on the cybersecurity requirements of the CIA triad between the interaction of VPP and power system. This subsection first categorizes existing cyberattacks into four main types: data theft, data tampering, service attacks, and unauthorized access, as detailed in Table II.

TABLE II
Categories of Existing Cyberattacks

Category	Specific technique	CIA	Typical target	Primary data type involved	Reference
Data theft	Traffic sniffing	C	Unencrypted network communication links	Directly acquired	[34], [35]
	Side-channel attack	C	Network communication links, terminal devices	Directly acquired	[34], [35]
Data tampering	False data injection	I	SCADA systems, EMS state estimation modules	Directly acquired, dispatching	[35]
	Demand manipulation	I	Power trading systems, VPP aggregator platforms	Trading, management	[36]
	Time synchronization	I	Network time protocol/precision time protocol (NTP/PTP) time servers	Dispatching	[37]
	Replay attack	I	Control commands for terminal devices	Dispatching	[38]
	Structured query language (SQL) injection attack	I	Backend databases	Trading, management	[39]
	Malicious routing attack	C, I	Routing devices in the communication network	Dispatching	[40]
Service attack	Distributed denial of service (DDoS)	A	Edge decision centers, communication links	Dispatching	[41]
	Delay attack	A	Time-sensitive control systems or protocols	Dispatching	
	Black hole attack	A	Routing devices in the communication network	Dispatching	[42]
	Primary-backup conflict	A	Edge computing gateways, servers on cloud platform	Dispatching	[43]
Unauthorized access	Malware	C, I, A	EMS platforms, VPP management platforms	All	[39]
	Phishing emails	C, I, A	Operation and maintenance laptops, email of employee	All	[44]
	Insider threat	C, I, A	Operation and maintenance laptops, system backends	All	[45]
	Password cracking	C, I, A	EMS platforms, VPP aggregation platforms	All	[46]

Data theft attacks primarily target the confidentiality aspect of the CIA triad, with the core objective of obtaining private data from demand-side users or the power system. Among common data theft methods, traffic sniffing targets unencrypted network communication links to directly intercept data. In contrast, side-channel attacks focus on encrypted channels or terminal devices, inferring private or encrypted data from indirect information such as the power consumption or processing time of the device, thereby enabling the deduction of sensitive information such as scheduling plans. Regarding these methods, [34] has verified the vulnerability of secure communication in smart grids to non-invasive side-channel attacks, even when protected by the advanced encryption standard. Specifically, it demonstrates that correlation electromagnetic analysis can successfully extract encryption keys from smart meters by analyzing leaked electromagnetic emanation during execution. This enables the unauthorized deduction of granular power consumption records, thereby exposing sensitive user behavioral patterns and operational data. Once a data theft attack succeeds, it not only violates user's data privacy (compromising confidentiality), but also exposes the operational strategies of VPPs and resource configurations, providing precise intelligence for subsequent and more destructive attacks.

Data tampering attacks primarily target the integrity aspect of the CIA triad. Their core objective is to alter critical data at any stage of the interaction of VPP with the power system (such as data acquisition, dispatching, or trading) to influence the quantity-price bidding curves of VPP aggregator or resource dispatching decisions. Among these attacks, the false data injection attack leverages the configuration information of the power system to inject forged measurement data into SCADA or VPP aggregation systems [35]. By constructing attack vectors that bypass traditional bad data detection mechanisms, the false data injection attack misleads the VPP aggregator into formulating dispatching or market strategies based on an incorrect estimation of system states. The demand manipulation attack [36] mainly alters the basic market trading information released by the trading platform from one day ahead, causing the VPP aggregator and other market entities to receive false price signals and disrupting market supply-demand balance by faking high electricity demand. The time synchronization attack [37] disrupts the high-precision time consistency of NTP/PTP protocols by injecting delays or forged synchronization messages, causing time discrepancies among devices on the network. This weakens the ability of VPP to perform services requiring rapid responses such as frequency regulation. The replay attack [38] intercepts and repeatedly retransmits resource control commands to interfere with the system execution state, thereby

causing disorder in the operational status of internal resources within the VPP. SQL injection attack, which exploits vulnerabilities in the management systems of VPP aggregators, allows attackers to maliciously alter core parameters and historical records stored in databases. By tampering with operational data such as transaction volumes and prices, these attacks directly compromise the integrity of inputs for bidding models, thereby distorting the formulated quantity-price curves formulated for future market participation [39]. Although the specific methods of these attacks vary, they all aim to compromise the data integrity, posing a significant threat to the validity of the decision-making of VPP and the operational security of power system.

Service attacks primarily threaten the availability aspect of the CIA triad. Their harm is mainly manifested by disrupting communication links, routing equipment, or server operations [40]. If successful, such attacks can paralyze the key network nodes or system platforms, preventing the VPP from providing required flexible regulation services in response to dispatching commands from power system operator. The most typical examples are traffic-based attacks aimed at exhausting network, computational resources, or communication bandwidth. These include DDoS attacks and various types of delay attacks, which inject a large volume of invalid access requests or artificially create network latency. This overloads bandwidth, central processing unit, or memory, thereby paralyzing communication links, edge computing gateways, and the aggregation platform. For communication protocols such as MQTT used in Internet of Things (IoT) architectures of VPP, [41] demonstrates that latency attacks can severely disrupt time-critical response services. By maliciously delaying the transmission of control data, such attacks cause distributed energy resources to exceed the second-level response windows required for frequency regulation, potentially leading to frequency oscillations or system destabilization. This category also includes attacks targeting network routing equipment and redundancy mechanisms. For instance, the black hole attack can forge routing updates to mislead devices like edge switches into directing data traffic to an unreachable "black hole" address [42].

The primary-backup conflict attack targets the redundancy mechanisms in high-reliability architectures. By faking primary device failure or manipulating status feedback, an attacker can bypass fault-tolerant configurations such as those employing redundant programmable logic controllers (PLCs) to trigger a premature failover. This creates a "split-brain" condition where conflicting commands are issued simultaneously, potentially driving the system into unsafe operating regions and leading to severe equipment failure [43]. The concept behind unauthorized access attacks differs from the previous three categories, which primarily target confidentiality, integrity, or availability individually. The main principle of this category is to directly steal credentials, either through password cracking (e. g., brute force attacks or implanting trojans to exploit system vulnerabilities) or social engineering (e.g., obtaining platform passwords directly from internal staff or using phishing to acquire low-level credentials). The primary targets are various application platforms or systems, and a successful attack can severely impact the CIA simultaneously. Reference [39] analyzes malware-induced cyberattacks within cyber-physical power system, demonstrating that infections can propagate silently during an incubation period before launching coordinated strikes. Taking the platform of the VPP aggregator as a target, once malware gains control authority over terminal nodes, attackers can maliciously trip power generation units or disrupt regulation processes. This directly compromises system integrity and availability, potentially leading to a significant loss of load and system paralysis [44]. An attacker could directly alter control strategies (compromising integrity), encrypt core data for ransom, or even issue a flood of incorrect control commands at a critical moment when the power system needs flexible regulation. Such threats are analogous to the "command error" contingencies in other cyber-physical systems, leading to system paralysis and endangering system security (compromising availability). Reference [45] indicates that social engineering allows attackers to bypass sophisticated technical defenses by exploiting human vulnerabilities. Through phishing emails that impersonate information technology (IT) support staff, attackers can deceive operations personnel into revealing login credentials. Once successful, they gain legitimate access to the backend management systems of VPP, posing a critical threat to the integrity and confidentiality of operational data and user's data.

B. Propagation of Cyberattacks and Potential Risk Analysis

A brief overview of the principles behind various cyberattacks is provided in Section III-A. In real-world scenarios, attackers typically do not employ a single attack method. Instead, they often start by exploiting a vulnerable node and then combine multiple attack methods to progressively expand the attack surface. Existing research has shown that cyberattacks targeting new entities such as VPPs are not static events isolated to a single node. Rather, they are complex processes that can dynamically propagate between the cyber information domain and the physical device domain. The impact of a cyberattack can also be amplified throughout the system in the form of cascading failures [46], [47].

This subsection aims to deconstruct the typical propagation paths of different cyberattacks within the four-layer functional hierarchy (cloud-tube-edge-terminal) to further analyze the real-world threats they may pose. Building upon the cybersecurity requirements identified for the operational workflows and communication architectures of VPP in the interactions with power system, this subsection adopts the four-layer functional hierarchy defined in Section II-C as a unified structure for analyzing cyber-risk propagation paths.

First, given that the distributed energy resources aggregated by VPPs are massive in scale, geographically dispersed, and characterized by highly heterogeneous communication protocols, conventional centralized cloud-based dispatching paradigms often encounter significant computational overhead and communication latency bottlenecks when managing highly time-sensitive services such as second-scale frequency response. By introducing an edge layer, the system can achieve localized data processing and protocol normalization

for heterogeneous resources. This hierarchical edge-decision structure and its associated technologies allow complex regulation logic to be decentralized to the resource proximity, thereby ensuring real-time operational performance while simultaneously facilitating data privacy protection [48]. Furthermore, research has consistently employed similar four-layer functional hierarchy to address the interactions of multi-energy flows and distributed control challenges involving heterogeneous resources (e. g., in integrated energy systems or microgrid clusters), demonstrating the representativeness and generalizability of this hierarchy in supporting various operational modes of interaction between distributed energy systems and the power system [49].

Second, the four-layer functional hierarchy effectively maps the cross-domain penetration process arising from the deep coupling of the information and physical layers of the power system. This hierarchy organically dissociates the network communication media (tube) of VPP from its local regulation loops (edge or terminal), providing a coherent analytical structure for deconstructing the evolution of attack vectors across different cybersecurity zones. Based on this, it is possible to illustrate how attackers exploit communication vulnerabilities between edge nodes and the core control layer to achieve vertical privilege escalation from the digital space to the physical execution layer or horizontal cross-zone penetration. This further reveals the underlying mechanisms by which malicious command tampering induces cascading failures in the power system [50]. Building on the analysis of the communication architecture and cybersecurity requirements of VPPs, the propagation paths of cyberattacks can be analyzed using a three-layer framework: the physical layer, the network layer, and the platform layer. The physical layer consists of the tangible application systems including distributed energy resources, lines, and controllable loads. The network layer comprises the communication networks and channels that support data transmission between different terminal devices, edge decision centers, and systems. The platform layer includes the application platforms and systems that perform functions such as resource monitoring, load forecasting, dispatch decision-making, and optimization control [51], [52]. The propagation of cyberattacks primarily manifests as horizontal penetration between these layers and vertical escalation across them.

The typical propagation paths of cyberattacks can be broadly categorized into three types.

Firstly, top-down platform penetration is a common path where attackers target application-layer platforms or corporate IT networks exposed to the public internet. After gaining access through methods like spear-phishing, the attacker can hijack the legitimate control channels of the platform to send malicious commands down to terminal devices at the physical layer, potentially causing large-scale power outages or physical equipment damage [53].

Secondly, in contrast, bottom-up terminal intrusion constitutes another typical path. Here, attackers select massive and less-protected physical devices (e.g., smart meters and PV inverters) as entry points. By compromising multiple local devices through methods such as man-in-the-middle (MITM) attacks or false data injection, they use these compromised devices as a springboard to upload deceptive information to the application layer. This misleads the system into making incorrect overall decisions, achieving the final attack objective through the cumulative impact of compromises across massive distributed devices [54].

Lastly, the most destructive propagation path involves exploiting the cyber-physical coupling between the network and physical layers to trigger cascading failures [55]. In this case, the attacker first launches an attack such as a DDoS or channel congestion attack at the network layer. This prevents the platform layer from receiving timely status information from critical lines at the physical layer. Alternatively, the attacker could infiltrate the higher network layers, specifically the wide-area network hosting SCADA and EMS, to alter control data or disable communication links. This disrupts the feedback loop between the edge and the cloud, rendering the platform-level systems incapable of monitoring or operating critical facilities, thereby creating an uncontrollable state within the physical layer [56]. If a power line is already operating under high load at this time, this loss of control could lead to line overloads. This initial physical fault would then cause a redistribution of power flow in the system, stressing other normal lines and triggering wider-scale physical overloads. This creates a vicious cycle where a network-layer failure leads to a physical-layer collapse that continuously self-amplifies [57]. Taking the cybersecurity zones stipulated under China's secondary cybersecurity protection codes within the four-layer functional hierarchy as an example, Fig. 3 illustrates these typical propagation paths of cyberattacks.

To systematically address these vulnerabilities, research has emphasized the necessity of establishing comprehensive cybersecurity frameworks for VPPs. Such frameworks are designed to safeguard the entire data interaction chain by prioritizing four critical cybersecurity objectives: information availability, operational reliability, protection against improper data alteration (integrity), and the maintenance of proprietary data confidentiality within IoT and cloud-based architectures [58]. References [59] and [60] evaluate cyberattacks across two dimensions: the technical complexity within the cloud-edge-terminal collaborative network and the resulting reliability impacts on the power system. Specifically, the heterogeneous nature of terminal devices and the dynamic environment of edge nodes significantly increase the difficulty of cross-layer execution, while the comprehensive impact on system stability can be quantified by modeling successful cyber penetrations as unexpected equipment outages. Through an analysis of these findings, it is evident that attack difficulty depends on the cybersecurity architecture of the target and the domain expertise of the attacker. For example, while SQL injection on public web platforms relies on relatively mature tools, achieving coordinated control over massive terminal devices through false data injection remains highly challenging. Such attacks require the adversary to possess adequate knowledge of power system operation and protection mechanisms to successfully manipulate state estimation and evade detection [61].

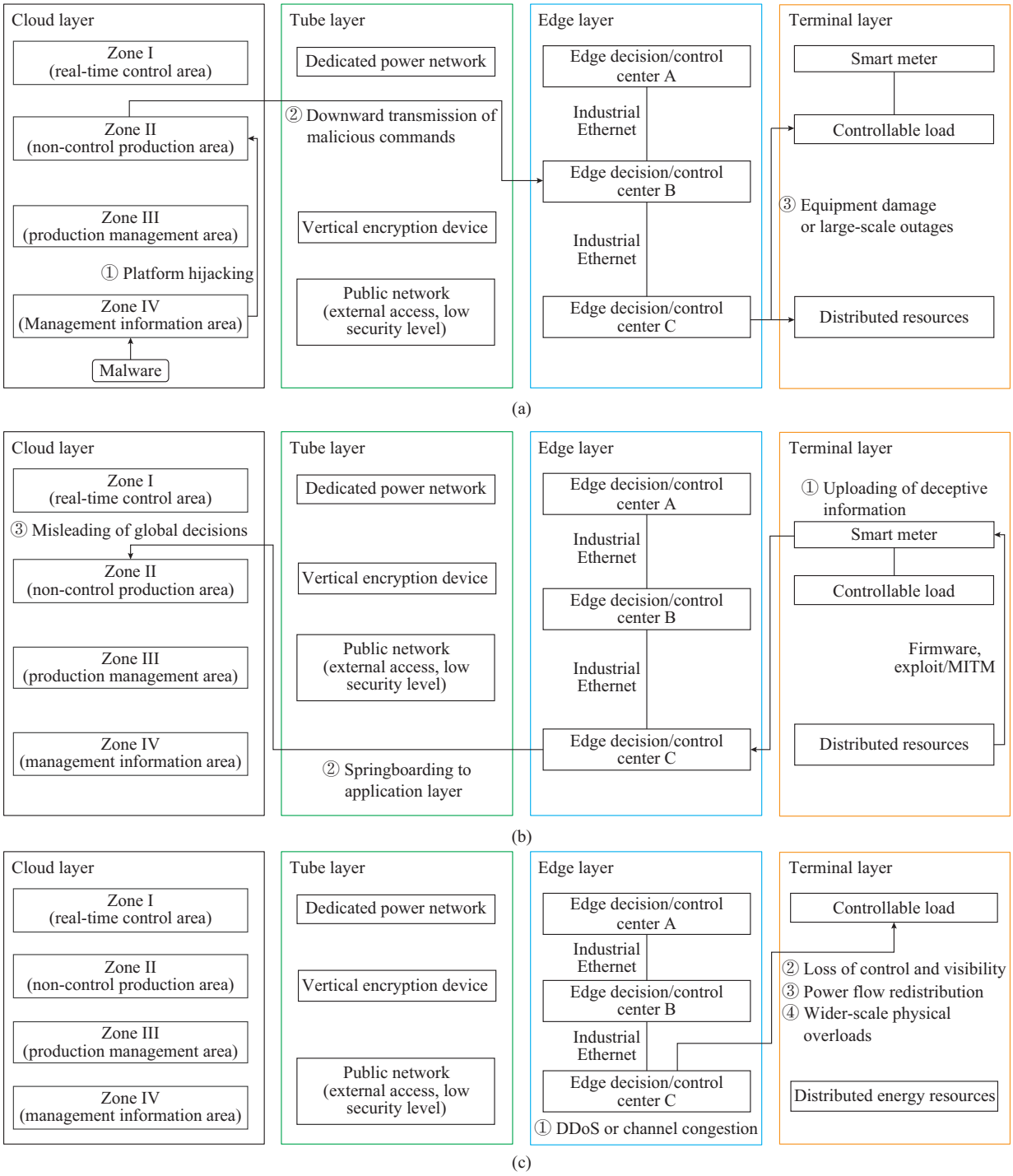

Fig. 3. Typical propagation paths of cyberattacks. (a) Top-down platform penetration. (b) Bottom-up terminal intrusion. (c) Cyber-physical coupling.

Additionally, the severity of the damage caused by the cyberattack needs to be evaluated by comprehensively considering impacts across different dimensions and aligning with the business processes of VPPs. First, regarding physical security impacts, the ultimate goal of an attack is to disrupt the secure and stable operation of the power system. For example, by exploiting the widespread vulnerabilities in terminal devices, an attacker can orchestrate massive IoT-based botnets to launch coordinated strikes. Within a VPP, such botnets can be utilized to execute a "simultaneous load injection" (a sudden and large-scale increase in demand) or a "simultaneous load withdrawal", creating artificial power fluctuations that trigger line overloads or frequency instability in the power system [62]. These artificially created large-scale power fluctuations can cause line overloads or voltage limit violations in the distribution network. In more severe cases, such cyberattacks can jeopardize the frequency stability of the power system, potentially triggering widespread blackouts. The severity of such damage can be precisely quantified using metrics such as load not served and system insta-

bility [63]. Second, in terms of economic consequences, an attacker can directly tamper with critical data such as bidding prices and settlement figures. Such non-control-data attacks are realistic threats that can corrupt decision and configuration data to achieve severe cybersecurity compromises without hijacking the control flow of the program. This not only inflicts direct financial losses on the VPP aggregator but may also lead to legal disputes due to the integrity violation of critical settlement data [64]. Finally, concerning social implications, the leakage of basic energy consumption data enables attackers to employ statistical models (e.g., machine learning) to infer sensitive private information, such as the daily routines of residential users or the production schedules of commercial enterprises. This erodes user trust in the VPP aggregator. In the event of a large-scale privacy data breach, it could even impede the commercial deployment and long-term growth of VPPs.

IV. Key Cybersecurity Defense Technologies for VPPs

Building upon the preceding analysis, this section focuses on the application boundaries of key cybersecurity defense technologies across various scenarios and provides an in-depth discussion on how the intrinsic attributes of VPPs dictate specific cybersecurity requirements. As previously noted, while each intrinsic attribute of AIR is intertwined with CIA threats, the primary cybersecurity demands for these attributes vary in the context of interaction of VPP with power system and evolving trends of defense. The specific analysis is as follows.

1) Aggregation: privacy protection and computational efficiency are the core requirements. Aggregation occurs at the forefront of the data chain, where the primary task is processing sensitive information from massive heterogeneous terminal devices. Given that real-time requirements are relatively flexible at this stage (typically on a daily basis, occurring before the actual operating day), the fundamental challenge for establishing a foundation of trust lies in utilizing robust data protection and cryptographic technologies to prevent unauthorized data access. Consequently, this section prioritizes the applicability of confidentiality-enhancing technologies such as anonymization, encryption, and foundational privacy-preserving computations in the aggregation phase.

2) Interaction: multi-party trust and communication link optimization are the core requirements. During market clearing and dispatch coordination, VPPs involve complex interest-based interactions among multiple stakeholders. The authenticity and integrity of data directly dictate the fairness of electricity trading and the scientific validity of dispatching decisions. The interaction phase focuses on utilizing key cybersecurity defense technologies such as blockchain to establish mutual-trust interaction chains among market participants, while simultaneously mitigating communication latency or signal loss resulting from limited bandwidth.

3) Regulation: real-time response and lightweight algorithms are the core requirements. In regulation phase at second or millisecond scales, any delay in command execution introduced by complex defensive logic or cybersecurity methods will directly impair the performance of VPP regulation, potentially triggering instability of the physical system. Therefore, defense at this stage must prioritize the control stability of the physical system, which restricts the implementation to lightweight cybersecurity mechanisms characterized by low latency. Adopting this business-priority-driven analytical logic allows for a clearer definition of the defensive boundaries for various cybersecurity defense technologies across the complex operational chain of VPP, while enabling the evaluation of their respective strengths, weaknesses, and application scenarios.

A. Typical Technologies and Application Scenarios

VPPs are facing numerous cybersecurity vulnerabilities and privacy leakage risks. A successful attack can severely impact the secure and stable operation of the power system. To ensure that VPPs can provide effective flexible regulation services to the power system, it is essential not only to enhance the cybersecurity of terminal devices and platforms [65], but also to carefully consider the data interaction methods across different communication links and deploy key cybersecurity defense technologies to prevent the escalation of single-node cyberattacks into systemic risks.

The working principles of different cybersecurity defense technologies vary slightly, but most operate by encrypting or transforming data, or setting access permissions to prevent attackers from directly accessing the unencrypted critical information. Among these, the most common technique is data anonymization, which typically operates at the level of sensitive fields. This includes methods such as replacing usernames with symbols, generalizing detailed addresses to broader regional areas, or adjusting data precision through differential privacy, thereby mitigating individual re-identification risks while keeping the underlying data structure intact [66]. Reference [67] validates this by introducing k-means clustering and an extreme gradient boosting based anonymization algorithm into a power data sharing scenario, and the results show that the anonymization algorithm effectively reduces data identifiability. However, data encrypted solely through field-level processing can still be re-identified when correlated with multi-source data. Therefore, some researchers have introduced masking algorithms, which use linear mapping or random perturbation to obscure individual information while preserving the overall statistical properties. Reference [68] proposes a masking algorithm based on linear mapping, and tests it in the day-ahead optimal dispatching of VPPs. The results show that the masked dispatching plan is unrecognizable in the cloud platform, but it is nearly identical to the original plan after de-masking, with a relative error of less than 10^{-4}, demonstrating the advantage of masking in balancing privacy and usability. Additionally, considering that locally encrypted data still face interception risks during cross-domain transmission, some researchers have applied a zero-sum noise algorithm to the transmission link. Its principle is to add noise to individual data points, ensuring that no valuable information can be obtained even if the data are intercepted. Reference [69] validates the zero-sum noise strategy in an economic dispatching scenario for

distributed energy resources, which only requires injecting noise during the initial iterations, and after that, it converges conventionally. The results prove its ability to defend against external eavesdropping and internal collusion inference attacks while maintaining the convergence performance. Overall, data anonymization technologies primarily focus on the data collection and transmission, serving as front-end protection in the end-to-end link of VPP.

Data anonymization and masking technologies serve as the primary defense technologies for VPPs to safeguard their aggregation attributes, typically deployed within the edge layer of the four-layer functional hierarchy. Their core logic involves erasing, replacing, or perturbing personally identifiable information or sensitive labels such as precise geographic coordinates and user's behavioral patterns, before the raw measurement data of distributed energy resources are uploaded to the tube layer. This mitigates the confidentiality leakage risks at the edge layer. However, the practical implementation of data anonymization is more complex than simple algorithmic deployment, as its effectiveness is often dictated by the multifaceted constraints of privacy security, data utility, and computational overhead [70]. Prioritizing the strength of data confidentiality in isolation inevitably compromises the statistical characteristics of raw load data. This results in a significant decline in data utility, providing aggregators with load information that is too coarse to support the fine-grained dispatching decisions on minute-to-second timescale.

In practice, VPPs face significant re-identification risks within big data environments. Even with preliminary anonymization, attackers may still infer the actual power consumption patterns of a user by correlating anonymized data with external and multi-source background knowledge such as public power system topologies or meteorological data. Consequently, practical deployments should move beyond reliance on single anonymization algorithms. Instead, metrics such as global certainty penalty or information loss must be introduced to dynamically and quantitatively evaluate the anonymization schemes. This ensures that resource-constrained edge terminals can achieve low-latency data processing while maintaining re-identification risks within acceptable safety thresholds.

During the trading, settlement, and data storage processes of a VPP, the data often need to be used in computations without being exposed in plaintext, making simple data de-identification methods insufficient for meeting the cybersecurity requirements. To address this, cryptographic primitives provide mechanisms for computation and verification on encrypted data. Unlike data anonymization, which converts original data into false and non-sensitive data, data encryption works by converting original data into unreadable ciphertext. HE is a classic example of this technology. It allows mathematical operations to be performed directly on ciphertext, enabling data manipulation and computation without decryption while preserving the CIA triad. In the context of VPPs, this supports privacy protection in distributed control and optimization tasks such as energy management and settlement, without exposing the original sensitive plaintext to the cloud or other participating entities [71]. Reference [72] combines the blockchain technology with HE to protect privacy in settling the electricity trading of VPP, and the results show that it could achieve a transparent revenue distribution mechanism with decryption results perfectly matching the plaintext. Reference [73] also uses HE in bid quantity protection, validating its efficiency and cybersecurity in large-scale node environments. However, even if data can be securely computed, if the encrypted information is stored centrally, it remains vulnerable to more advanced cyberattacks. Consequently, some researchers have proposed secret sharing schemes, often integrated with blockchain consensus protocols such as Raft to decentralize the data aggregation process. By leveraging the additive homomorphic property of secret sharing, sensitive data can be split into multiple shares for distributed processing without relying on a trusted central authority. The original data can only be recovered when a specific threshold of shares is met, thereby enhancing the cybersecurity during storage and trading [74]. Reference [75] uses Shamir's secret sharing scheme in the optimization of internal transaction decision of a VPP, demonstrating its effectiveness in preventing information tampering and protecting the privacy of VPP aggregator. Furthermore, even if the data are securely stored and computed, the communication process must be protected against forgery and tampering. Therefore, some researchers have introduced digital signature technology into VPP business processes. It relies on elliptic curve cryptography (ECC) to achieve message authentication and non-repudiation, ensuring the authenticity and trustworthiness of transmitted content [76]. Reference [77] reviews the applicability of encryption technologies such as Rivest-Shamir-Adleman algorithm and ECC in VPP trading. It is concluded that ECC offers a better balance of performance and cybersecurity, making it suitable for the real-time trading and data authentication of VPPs.

Cryptographic methods serve as the core pillar for securing the VPP aggregation and interaction processes, primarily applied to data transmission in the tube layer and privacy processing in the edge and cloud layers. They aim to ensure that control commands remain tamper-proof during transit across unsecured networks while simultaneously safeguarding the confidentiality of sensitive power consumption data during aggregation. Taking HE, the most widely utilized technique in this category as an example, a critical trade-off between operational logic compatibility and computational depth constraints exists during its application in VPPs. On one hand, while HE allows logical operations directly on ciphertext, mainstream VPP dispatching prediction algorithms such as artificial neural networks rely on non-linear activation functions, which conflict with the algebraic characteristics of HE that support only polynomial addition and multiplication. On the other hand, the bootstrapping operation in HE, used to refresh ciphertext noise and support infinite-depth calculations, suffers from inherent flaws such as extreme computational overhead and high latency, making it entirely incompatible with the high-frequency dispatching interaction requirements of VPPs. Consequently, semi-HE schemes without bootstrapping are predominantly adopted in engineering practice. However, these methods are limited by

fixed multiplicative depths, which constrains the implementation of complex and multi-round iterative optimization algorithms for VPPs.

In practice, the computational depth constraints of HE dictate that VPPs must achieve a balance between operational and cryptographic requirements through algorithmic reconstruction. Empirical research in [78] demonstrates that by replacing traditional deep learning models with the Ivakhnenko group method of data handling (GMDH) based on quadratic polynomials, ciphertext load forecasting can be achieved without exposing the privacy of individual household. In terms of performance, for a micro-VPP consisting of 10 households, parallelized ciphertext prediction takes approximately 4 s, whereas sequential processing requires nearly 30 s. Latency of this magnitude indicates that HE is currently only viable for engineering applications in market trading and day-ahead scheduling, where the response time is measured in minutes. To support real-time regulation tasks (e.g., secondary frequency regulation) that demand millisecond-level responses, significant breakthroughs in hardware acceleration or algorithmic lightweighting remain necessary.

As the scale of distributed energy resources grows and market trading mechanisms evolve, VPPs can aggregate a wider range of heterogeneous resources and respond to the differentiated control requirements of transmission and distribution systems. However, this expansion imposes stringent demands on the computational efficiency and accuracy of the AIR models. Researchers have found that encrypting data and decrypting them before computation can affect the computational efficiency and accuracy to some extent, making it difficult to support complex tasks with high timeliness requirements. To address this practical need, privacy-preserving computation enables joint training and decision-making without exposing raw data, providing a privacy foundation for cross-domain collaboration and complex optimization in VPPs. Among these technologies, federated learning (FL) is well-suited to the business of VPPs. It allows edge decision-making entities to complete model training locally and only upload the trained parameters for global aggregation. This enables the sharing of modeling results while avoiding the centralized exposure of raw data. Reference [79] uses an FL framework for VPP load forecasting and achieves joint modeling of multi-regional VPPs, which can improve the prediction accuracy while ensuring privacy. Reference [80] introduces FL into the optimization of community renewable energy consumption, verifying its feasibility and privacy advantages in cross-domain optimization. However, in large-scale computations involving transaction settlement and resource dispatching optimization, the transmission of numerous intermediate calculation parameters still poses a cybersecurity risk of being cracked by cyberattacks. Therefore, multi-party computation (MPC) has been introduced, allowing participants to jointly compute the result of a target function without revealing their individual inputs and outputs. Reference [81] proposes a privacy-preserving hierarchical game model based on MPC, proving its effectiveness in market game scenarios. Reference [82] applies the applications of MPC to privacy-preserving power flow analysis, enabling the secure evaluation of power system operating conditions among distributed prosumers. Additionally, differential privacy injects noise into data or model updates to weaken the inference capabilities of an attacker, further reducing the risk that an attacker can infer individual user data from model update information. Reference [83] uses a differential privacy mechanism to perturb VPP dispatching data, and the results show a significant enhancement in data protection with controllable error levels. Finally, when the cybersecurity of the operating environment itself is in doubt, a trusted execution environment can be established to provide hardware-level isolation and protection, ensuring the integrity and trustworthiness of code and data during execution [84].

Privacy-preserving computation technologies such as FL and MPC are central to achieving collaborative optimization of large-scale heterogeneous resources in VPPs, primarily operating at the interaction interface between the edge and cloud layers. These technologies are designed to safeguard the confidentiality of the VPP aggregation and interaction attributes, enabling participants to jointly train the dispatching prediction models without exposing raw power consumption data. The primary challenge in VPP applications of these technologies lies in the conflict between privacy protection gain and communication resource consumption. Although FL avoids direct leakage of raw data, its model training process involves high-frequency and bidirectional exchange of parameter gradients between massive heterogeneous terminals and central servers. When a VPP aggregates massive residential-side devices, this communication bottleneck can lead to severe congestion in the communication links of the tube layer. Furthermore, the non-independent and identically distributed (Non-IID) characteristics of VPP terminal data, where power consumption habits vary significantly among users, can lead to slow convergence in traditional FL models and even trigger instability in the outputs of aggregation algorithm.

To address these issues, a selective update mechanism must be introduced in practical engineering applications of privacy-preserving technologies to optimize the communication overhead. For instance, [85] demonstrates that adopting a cluster-analysis-based FL (CA-FL) architecture can significantly enhance system efficiency when dealing with the heavy communication loads generated by edge nodes. The underlying logic is to identify and upload only representative local model updates rather than the full gradients from all nodes. Experimental results indicate that this improved cluster-analysis-based FL architecture effectively reduces network bandwidth occupancy while maintaining model accuracy, demonstrating greater robustness than traditional FL when processing Non-IID data such as the heterogeneous load characteristics. This implies that in VPP environments with limited tube-layer bandwidth or high sensitivity to communication costs, this selective transmission-based privacy-preserving computation paradigm offers higher practical value for engineering deployment.

In addition to the three categories of data anonymization, cryptographic methods, and privacy-preserving computation, another category of key cybersecurity defense technologies

focuses on data usage permissions, specifically implemented through access control and key distribution. Here, the security of data usage is emphasized. Its core logic is to progressively refine access boundaries on top of data encryption, effectively solving the permission allocation problems in cross-domain sharing and multi-party collaboration. A typical application is attribute-based encryption, which establishes a cryptographic mapping between user attributes and access policies, permitting decryption only by users whose attributes satisfy the specified policy criteria. This achieves differentiated allocation of data permissions during data sharing [86]. Reference [87] proposes a method combining distributed attribute-based encryption and attribute-hiding zero-knowledge proof, validating its efficiency in multi-scenario data sharing of VPP (e. g., transactions and queries). The results show that the proposed method achieves data indistinguishability and tamper-proofing while maintaining low computational costs and system overhead even at high request frequencies. Furthermore, by establishing access control or identity authentication mechanisms based on role, attribute, and certificate systems, permissions of user's behavior can be restricted more granularly. The introduction of multi-factor authentication also reduces the risk of unauthorized access due to identity forgery [88]. Reference [89] proposes a comprehensive cybersecurity defense system that combines blockchain, privacy-preserving computation, and identity authentication throughout the entire process of VPP trading. The results show that this system effectively addresses issues such as heavy identity authentication burdens and unauthorized access, and has been validated in several domestic and international demonstration projects such as the Brooklyn Microgrid Project in the USA and the Large-scale Flexible Resource VPP Trusted Trading Demonstration Project in China. Meanwhile, [90] validates a zero-trust architecture in a VPP. By adopting the principle of least privilege, continuous trust monitoring, and micro-segmentation, this architecture achieves strict control over device and user's access. The results indicate that this architecture can effectively defend against internal attacks and unauthorized access risks, providing a system-level complement to multi-factor authentication logic.

Secure communication and access control serve as the physical boundaries of the VPP defense system, primarily deployed at the tube and terminal layers. Their core task is to safeguard the availability and authenticity of regulation commands, ensuring that only authorized aggregation platforms can issue physical action instructions to underlying heterogeneous resources.

Currently, VPPs face a critical conflict between authentication depth and regulation delay in real-time control environments. Traditional identity authentication protocols are predominantly based on "one-to-one" handshake mechanisms. When an aggregator requires millisecond-level frequency regulation for massive regional distributed energy resources, the cumulative delay from establishing individual secure sessions can lead to command failure or even trigger instability in the physical power system. Furthermore, many underlying terminal devices such as low-end sensors possess extremely limited computational capacity, making them unable to support the memory occupancy required by heavy asymmetric encryption algorithms. To resolve these issues, the introduction of one-to-many authentication and lightweight cryptographic primitives is essential. Referring to the framework proposed in [91], utilizing Hash functions and authenticated encryption primitives can significantly reduce the computational overhead when addressing the challenges of concurrent access from massive terminals in IoT environments. Empirical results demonstrate that this one-to-many mechanism allows aggregators to establish secure keys with multiple terminals simultaneously in a single session, drastically compressing the communication round-trip time (RTT). This lightweight concurrent authentication provides a feasible engineering path for VPPs to balance identity verification strength with real-time response speed in resource-constrained edge environments, ensuring that regulation commands arrive at physical actuators on time under verified cybersecurity.

Cross-domain transactions and multi-party collaboration in VPPs involve a large number of participants and often lack a unified central authority. It is insufficient to rely solely on encryption and access control for resolving the fundamental problem of mutual distrust among these parties. To address this challenge, in addition to the aforementioned methods, blockchain and smart contract technologies have been increasingly adopted to establish a robust trust mechanism in trading processes involving multiple market entities including VPPs. The essence of blockchain technology is to establish data trustworthiness through a decentralized ledger, consensus mechanisms, and tamper-proof features, providing guarantees of immutable and traceable data storage and transactions. Reference [92] introduces a blockchain architecture into a market-based trading platform for VPPs and verifies its effectiveness in preventing transaction data tampering and ensuring settlement transparency. While blockchain technology can be applied across the entire data lifecycle, automating the execution of VPP market transactions in a multi-party game environment requires reliance on smart contracts. A smart contract represents a self-executing protocol stored on the blockchain that is automatically triggered when preset conditions are met, thereby minimizing human intervention and susceptibility to manipulation. Reference [93] builds a smart contract based on Hyperledger Fabric to automate the execution of VPP economic dispatch and secure transactions. Similarly, [94] proposes a VPP dispatching model based on smart contracts that achieves automatic rule triggering and settlement, with experiments demonstrating its capability to enhance the operational efficiency and transaction fairness in a multi-party game environment.

Blockchain and smart contract technologies provide a decentralized trust foundation for VPPs, primarily deployed at the interaction interface between the cloud and tube layers. Their core value lies in safeguarding data integrity and non-repudiation within the interaction attribute, particularly during the economic settlement phase of double-auction markets involving distributed energy resources. However, VPP opera-

tions involve high-frequency cross-entity interactions among massive heterogeneous distributed energy resources, whereas the redundant consensus mechanisms of traditional blockchain significantly increase the interaction latency. This renders them incompatible with the real-time requirements for interaction between VPPs and the power system, e.g., secondary frequency regulation. Furthermore, the transparency of blockchain ledgers poses a significant challenge in electricity market scenarios: attackers may employ inference attacks to analyze on-chain transaction data and reverse-engineer sensitive VPP regulation strategies or commercial user's privacy.

To address the core bottlenecks of traditional blockchain architectures, optimized structures integrating sharding consensus and hybrid privacy mechanisms have emerged as a frontier for enhancing the engineering applicability of blockchain in various VPP scenarios. According to [95], adopting sharding consensus strategies to select validation nodes can effectively overcome the throughput limitations of single chains, significantly improving the efficiency of auctioning and execution in bilateral trading. Meanwhile, introducing the Rényi differential privacy algorithm into the consensus process to anonymize sensitive data achieves flexible and full-link privacy protection at a lower computational cost. Empirical data indicate that this algorithm not only enhances concurrent processing capabilities but also reduces the average power consumption during VPP operations by approximately 54.64%, which proves that through algorithmic dimensionality reduction and consensus partitioning, blockchain technology can satisfy the dual requirements of cybersecurity and engineering efficiency in cross-entity VPP interactions.

Based on the systematic review and analysis, a summary of the aforementioned key cybersecurity defense technologies and their typical applications are provided in Table III.

TABLE III
MAINSTREAM KEY CYBERSECURITY DEFENSE TECHNOLOGIES AND THEIR TYPICAL APPLICATIONS

Category	Specific technique	Working principle	Protection stage	Pros	Cons	Reference
Data de-identification	Data anonymization	Replace or generalize sensitive fields to hide user identity	Data collection and pre-upload	Low overhead and suitability for static data	High re-identification risk and utility loss	[66], [67]
	Perturbation algorithm	Mask data via linear mapping or noise while preserving statistical properties	Data collection and pre-upload	Rigorous privacy and flexible noise addition	Trade-off between privacy and data accuracy	[68]
Cryptographic methods	HE	Enable direct mathematical operations (addition or multiplication) on ciphertext	Trading, settlement, and optimization stages	Protection of data during aggregation	High computational or communication overhead	[71]-[73]
	Secret sharing	Split data into fragments, and original data requires a threshold number of shares to rebuild	Data storage and trading stages	No single point of failure	High overhead for share distribution or reconstruction	[74], [75]
	Digital signature	Use elliptic curve cryptography to sign and verify messages against tampering	Communication and trading stages	Strong integrity and non-repudiation	Complex key management and heaviness for edge devices	[76], [77]
Privacy-preserving computation	FL	Train models locally, and only upload parameter updates for central aggregation	Data training and computation stages	Raw data remaining local and reduction of transmission	Vulnerability to poisoning attacks and non-IID data issues	[78], [79]
	MPC	Multiple parties jointly compute a function without revealing private inputs	Collaborative dispatching and settlement stages	Secure computation without trusted third parties	High latency and poor scaling with many participants	[80], [81]
	Differential privacy	Inject noise into data/models to prevent individual information reconstruction	Data sharing and training stages	Strong mathematical privacy guarantees	Strict trade-off between privacy budget and utility	[82]
	Trusted execution environment	Utilize hardware-based secure areas to isolate code and data during execution	Local computation and data processing stages	High-performance hardware isolation	Hardware dependency and vulnerability to side-channels	[83]
Secure communication and access control	Attribute-based encryption	Grant decryption access only to users matching specific attribute policies	Data transmission and access sharing stages	Fine-grained access control	Costly decryption and complex key management	[86], [87]
	Access control and identity authentication	Restrict access based on roles/certificates, often via multi-factor authentification	Data sharing and communication stages	Fundamental and wide applicability	Complexity of managing massive heterogeneous devices	[88]-[90]
	Zero-sum noise algorithm	Add noise during transmission, keeping overall statistics valid while masking points	Data transmission stage	Simplicity of implementation for aggregation	Vulnerability to internal collusion attacks	[69]
Blockchain and smart contracts	Blockchain	Establish decentralized trust via distributed ledgers and consensus mechanisms	Entire data lifecycle	Immutable ledger and decentralized trust	Low throughput and high storage/latency limits in real time	[92]
	Smart contract	Encode trading or dispatch rules onto the blockchain for automated execution	Trading and dispatching stages	Automated and tamper-proof execution and elimination of intermediary trust	Difficulty to modify after deployment, bounded by blockchain throughput	[93], [94]

B. AI-based Defense Technologies

The continuous evolution of AI provides novel solutions for user's data privacy, establishing itself as a pivotal future direction. A primary application of AI in cybersecurity involves leveraging massive volumes of resource user's data to actively learn historical patterns and model the non-linear relationships between different variables, thereby facilitating the proactive perception of abnormal data in terminal devices, communication links, and system platforms. For example, graph neural networks (GNNs) can represent both the physical layer (including distributed PV, electric vehicles, and other terminal devices, as well as the distribution network topology) and the network layer as a unified graph structure to capture the collaborative operational characteristics across nodes. When an attacker simultaneously injects low-magnitude false data into multiple PV inverters that are geographically close, the local measurements at each node may not exhibit significant abnormalities. However, from the perspective of the overall network structure and regional operational patterns, the statistical characteristics of these measurements will deviate from normal spatial correlations. Leveraging this characteristic, GNNs can identify the potential threat and trigger an alarm [96].

While effective, these anomaly detection methods remain inherently reactive, addressing threats only after they manifest, by which time a cyberattack may have already impacted power system operations or compromised user's privacy. To overcome this limitation of passive defense, AI applications are pivoting toward active defense that orchestrates cybersecurity through intelligent predictive assessment utilizing predictive analytics. Active defense mines historical attack data, network traffic, and system logs to identify existing cybersecurity vulnerabilities within the system, or to predict the correlated features of future attacks. Research has shown that machine learning models such as random forest, gradient boosting, and neural networks can effectively predict cyberattacks. By analyzing key indicators such as source IP addresses, packet sizes, and malicious traffic, these models can assess the likelihood of an attack in advance [97]. Furthermore, active defense now extends to the early stages of the software development lifecycle. For instance, emerging technologies such as large language models (LLMs) are now being applied to code-level automated vulnerability assessment. Unlike traditional static analysis tools that rely on predefined rules, LLMs can understand the contextual logic and semantics of code more deeply, enabling them to identify more complex and hidden cybersecurity flaws before the code is integrated (e.g., during a change of request), thereby eliminating potential threats at the source side [98].

To transition the defense from static prediction to dynamic rehearsal, an advanced and proactive AI-driven defense technology has been realized through the integration of digital twin. The core of digital twin lies in constructing a high-fidelity and dynamic virtual counterpart of a physical system or a complex network environment. Within this secure virtual environment, simulation drills of various high-intensity cyberattacks can be carried out targeting any stage of the interaction of VPPs with the power system to verify the vulnerabilities of different systems, terminals, and communication links in realistic cyberattack scenarios. In related studies, researchers have successfully built digital twin models for infrastructure such as hydropower plants. By simulating industrial control protocol attacks on the twin, they can precisely quantify the specific impact of the attack on characteristic parameters of the hydropower plant, such as power generation outputs and water flow rates [99]. This quantitative assessment method allows the effectiveness of key cybersecurity defense strategies to go beyond theoretical analysis. Instead, these strategies can be repeatedly tested, compared, and optimized in the twin environment. Ultimately, the empirically validated AI detection models can provide the VPP architecture with preemptive foresight, facilitating a fundamental transition from traditional passive defense to data-driven active defense.

However, the deployment of AI also introduces endogenous security risks inherent to the models themselves. A critical concern is the susceptibility to "adversarial example attacks" during the inference phase. Within the business processes of VPPs participating in power system interaction, sophisticated attackers can inject imperceptible perturbations into real-time telemetry data (e. g., voltage readings or price signals). As demonstrated in [100], these adversarial examples are designed to mislead AI-based anomaly detection systems into misclassifying malicious cyberattacks as benign grid fluctuations, thereby bypassing the defense perimeter. Beyond the inference phase, the training phase is also vulnerable to "poisoning attacks". As analyzed in [101], attackers can employ generative adversarial networks (GANs) to construct synthetic and "clean-label" poison data. When injected into the FL process of a VPP, these malicious samples can corrupt the convergence of the global model without triggering traditional alarms. To counter these dual threats, VPP operators must implement defense technologies such as adversarial training for model robustness and data washing algorithms to filter out malicious noise from the training datasets.

C. Challenges and Development Trends of Cybersecurity in VPPs

Based on the preceding analysis of intrinsic attributes of VPPs, endogenous security drivers, potential attack risks, and key cybersecurity defense technologies, the core challenges currently facing cybersecurity in VPPs are summarized as follows.

1) The conflict between real-time regulation demands and the computational overhead of robust security algorithms. The flexible regulation capabilities of VPPs require aggregator platforms to respond to grid frequency and voltage fluctuations within second-to-millisecond intervals. However, as previously analyzed, advanced privacy-preserving technologies such as HE and MPC introduce substantial computational burdens and communication latencies. Striking an optimal balance between cybersecurity strength and real-time operational performance remains a critical technical bottleneck. This challenge is particularly acute because underlying edge-side terminals such as smart meters and low-power IoT gate-

ways possess highly constrained processing power and memory, rendering them incapable of executing resource-intensive cryptographic operations on millisecond time scales.

2) The fragmentation of massive heterogeneous terminal devices and the challenges of consistent standard management for cybersecurity. VPPs aggregate diverse end devices from various manufacturers adhering to different protocols. As discussed previously, these devices exhibit significant disparities in physical performance, firmware security, and patch update capabilities. Even with customized defense adaptations for specific scenarios, establishing a unified cybersecurity trustworthiness evaluation metric system and achieving efficient authentication and vulnerability monitoring across massive heterogeneous nodes throughout their lifecycle remain challenging. This is essential to prevent such nodes from serving as logical springboards for cross-domain penetration and to ensure the overall consistency of system-wide defense.

3) The conflict between data privacy and traceability of cross-domain business chain in multi-party interaction environments. The interaction attribute of VPPs involves multiple stakeholders including power system operators, aggregators, third-party service providers, and end-users. While blockchain technologies offer advantages in quantifying data integrity through immutability, distributed consensus, and full-link traceability, an inherent trade-off exists between the depth of data sharing (privacy protection) and business chain traceability (audit compliance) within complex power market dynamics. Current defense mechanisms lack standardized collaborative frameworks capable of balancing data utility metrics with privacy protection strength, especially when addressing targeted advanced persistent threats and insider threats.

Furthermore, based on the industry demands for cybersecurity in VPPs and current technical hotspots in the power and communication sectors, the development trends for key cybersecurity defense technologies are summarized as follows.

1) Evolution from passive defense toward an integrated active defense architecture. Future VPP frameworks will transcend reactive threat mitigation to establish an integrated system that comprehensively secures the entire operational lifecycle. This architecture, centered on multimodal large cybersecurity models and distributed multi-agent reinforcement learning, leverages domain-wide network situation awareness to facilitate proactive risk assessment and prediction, enabling the precise identification of various cyberattack methods [102]. Furthermore, by integrating software-defined networking and digital twin technologies, the system can achieve systemic self-healing through the dynamic isolation of compromised nodes and autonomous reconfiguration of communication paths, marking a systemic transition from single-point passive monitoring to proactive threat intelligence.

2) A lightweight collaborative defense system tailored for edge-intelligent decision-making. To meet the engineering requirements of VPPs, where edge-side computational resources are limited and operations are highly time-sensitive, the focus of cybersecurity defense technologies is pivoting from cloud-centric processing models (characterized by centralized bulk data uploading) toward a distributed paradigm based on autonomous edge-node decision-making. Future trends will prioritize the development of lightweight cybersecurity algorithms for edge gateways and smart terminals. By utilizing tiny machine learning (TML) along with techniques such as model pruning, quantization, and distillation, these systems can achieve high-precision attack detection while significantly reducing computational overhead and memory occupancy [103]. This edge-decision paradigm enables VPPs to identify and intercept local anomalous commands within milliseconds without relying on cloud-layer links, achieving deep coupling between the defense and operational response.

3) Firmware-level embedding and endogenous security for massive heterogeneous terminals. Addressing the challenges of fragmented terminal models, outdated cybersecurity protocols, and the difficulty of hardware replacement among aggregated distributed energy resources, the focus of defense is shifting toward firmware-level endogenous security hardening. Future development involves creating lightweight and portable embedded cybersecurity modules that reconstruct the logical core of terminal firmware. This provides unified identity authentication and data encryption interfaces for both legacy and new heterogeneous devices without requiring specific hardware architectures [104]. Such soft-embedding technologies can patch security vulnerabilities at the lowest level of physical execution, bridging the defensive gaps caused by inconsistent manufacturer standards.

V. Conclusion and Outlook

To address the cybersecurity defense requirements in the development of VPPs, this paper constructs a cybersecurity theoretical framework for VPPs, which is achieved by analyzing the intrinsic attributes of VPPs, i.e., AIR, and integrating them with the principles of the CIA triad. Within this framework, this paper outlines the business processes and data interaction methods for VPPs participating in power system interaction, analyzes potential cyberattack vulnerabilities and their impacts, and summarizes the categories and working principles of key cybersecurity defense technologies. This paper can serve as a reference for in-depth research on the cybersecurity in VPPs.

Furthermore, the advancement of AI offers a novel method to address the privacy protection requirements of VPPs and their aggregated resources, but several technical challenges must be overcome before the application at scale. On the one hand, AI-based real-time privacy protection requires massive amounts of data and significant computational power, which somewhat increases the configuration and operational costs for VPP aggregators. On the other hand, AI models suffer from a lack of interpretability. They are also vulnerable to adversarial examples, which can be introduced by attackers during the training process to disrupt decision-making parameters and lead to critical failures in key scenarios. Therefore, how to integrate AI with the practical characteristics and business needs of VPPs will be a key direction for developing low-cost solutions to user's privacy protection

capable of countering constantly evolving cyberattacks.

REFERENCES

[1] S. Shahzad and E. Jasińska, "Renewable revolution: a review of strategic flexibility in future power systems," *Sustainability*, vol. 16, no. 13, p. 5454, Jun. 2024.

[2] C. Hui, H. Zhang, and Z. Wang, "A review of market and scheduling characteristic parameter aggregation algorithm of different types of virtual power plants," *Proceedings of the CSEE*, vol. 43, no. 1, pp. 15-27, Jan. 2023.

[3] H. Gao, C. Kang, J. Li *et al*., "Analysis of technological evolution and operational challenges for virtual power plants in new power systems," *Transactions of China Electrotechnical Society*, vol. 40, no. 19, pp. 6057-6071, Oct. 2025.

[4] Q. Chen, H. Gao, C. Feng *et al*., "Dynamic construction and trustworthy quantification of virtual power plant: theoretical analysis and key technologies," *Automation of Electric Power Systems*, vol. 46, no. 18, pp. 26-36, Sept. 2022.

[5] I. Arghire. (2020, Jul.). Ransomware operators demand $14 million frompower company. [Online]. Available: https://www. securityweek. com/ransomware-operators-demand-14-million-power-company

[6] N. Naval and J. M. Yusta, "Virtual power plant models and electricity markets – a review," *Renewable and Sustainable Energy Reviews*, vol. 149, no. 10, p. 111393, Oct. 2021.

[7] E. A. Bhuiyan, M. Z. Hossain, S. M. Muyeen *et al*., "Towards next generation virtual power plant: technology review and frameworks," *Renewable and Sustainable Energy Reviews*, vol. 150, no. 10, p. 111358, Oct. 2021.

[8] H. Gao, T. Jin, C. Feng *et al*., "Review of virtual power plant operations: resource coordination and multidimensional interaction," *Applied Energy*, vol. 357, p. 122284, Mar. 2024.

[9] F. Marzbnal, A. Osman, and M. S. Hassan, "Advances in virtual power plant operations: a review of optimization models," *IEEE Access*, vol. 13, no. 13, pp. 131525-131548, Jul. 2025.

[10] S. Yang, K. Lao, H. Hui *et al*., "Secure frequency regulation in power system: a comprehensive defense strategy against FDI, DoS, and latency cyber-attacks," *Applied Energy*, vol. 379, p. 124772, Feb. 2025.

[11] Z. Yin, S. Wang, and Q. Zhao, "A flexibility scheduling method for distribution network based on robust graph DRL against state adversarial attacks," *Journal of Modern Power Systems and Clean Energy*, vol. 13, no. 2, pp. 514-526, Mar. 2025.

[12] M. A. Ferrag, L. A. Maglaras, H. Janicke *et al*., "A systematic review of data protection and privacy preservation schemes for smart grid communications," *Sustainable Cities and Society,* vol. 38, no. 4, pp. 806-835, Apr. 2018.

[13] L. Dias and T. A. Rizzetti, "A review of privacy-preserving aggregation schemes for smart grid," *IEEE Latin America Transactions*, vol. 19, no. 7, pp. 1109-1120, Jul. 2021.

[14] A. Bhoomadevi, P. L. Soundarraj, V. Gupta *et al*., "Security and privacy in internet of things (IoT) environments," in *Proceedings of IEEE 9th International Conference on Science, Technology, Engineering & Management*, Chennai, India, Apr. 2024, pp. 1-6.

[15] B. Zhou, H. Gao, R. Cheng *et al*., "Technical system construction for virtual power plants from first principles perspective," *Automation of Electric Power Systems*, vol. 49, no. 20, pp. 3-15, Oct. 2025.

[16] Y. Yang, M. Bao, Y. Ding *et al*., "Review of information disclosure in different electricity markets," *Energies*, vol. 11, p. 3424, Dec. 2018.

[17] O. Tsvilii, "Cybersecurity regulation: cybersecurity certification of operational technologies," *Technology Audit and Production Reserves*, vol. 1, no. 2, pp. 54-60, Feb. 2021.

[18] Q. Wu, C. Li, and J. Bai, "Optimal bidding strategy for multi-energy virtual power plant participating in coupled energy, frequency regulation and carbon trading markets," *International Journal of Hydrogen Energy*, vol. 73, no. 7, pp. 430-442, Jul. 2024.

[19] Y. Zhang, H. Zhao, and B. Li, "Distributionally robust comprehensive declaration strategy of virtual power plant participating in the power market considering flexible ramping product and uncertainties," *Applied Energy*, vol. 343, p. 121133, Aug. 2023.

[20] S. W. Ryu, S. I. Moon, and G. S. Lee, "Data-driven optimal bidding algorithm for VPP using polynomial regression model: actual case study of Jeju island," *IEEE Access*, vol. 13, no. 13, pp. 195657-195672, Oct. 2025.

[21] H. Pandžić, I. Kuzle, and T. Capuder, "Virtual power plant mid-term dispatch optimization," *Applied Energy*, vol. 101, pp. 134-141, Jan. 2013.

[22] T. Ding, J. Lv, R. Bo *et al*., "Lift-and-project MVEE based convex hull for robust SCED with wind power integration using historical data-driven modeling approach," *Renewable Energy*, vol. 92, no. 7, pp. 415-427, Jul. 2016.

[23] T. Zang, S. Wang, Z. Wang *et al*., "Integrated planning and operation dispatching of source-grid-load-storage in a new power system: a coupled socio-cyber-physical perspective," *Energies*, vol. 17, no. 12, pp.3013, Jun. 2024.

[24] T. Yang, J. Wang, Y. Liang *et al*., "Economic dispatch between distribution grids and virtual power plants under voltage security constraints," *Energies*, vol. 17, no. 1, pp. 117, Jan. 2024.

[25] X. Wei, S. Pan, B. Wang *et al*., "Review on virtual power plant resource aggregation and collaborative regulation using cloud-tube-edge-end architecture," *Journal of Global Energy Interconnection*, vol. 3, no. 6, pp. 539-551, Dec. 2020.

[26] SunSpec Alliance. (2025, Feb.). SunSpec Modbus for DER information model. [Online]. Available: https://sunspec.org/wp-content/uploads/2025/01/SunSpec-DER-Information-Model-Specification-V1-2.pdf

[27] National Institute of Standards and Technology. (2026, May). NIST framework and roadmap for smart grid interoperability standards. [Online]. Available: https://www.nist.gov/ctl/smart-connected-systems-division/smart-grid-group/smart-grid-framework/framework-and-road-map

[28] *MQTT Version 5.0*, OASIS Standard, 2019.

[29] M. Sawilam, B. Kizilkaya, D. Flynn *et al*., "A secure and scalable architecture for virtual power plants inspired by VPN principles," in *Proceedings of 2025 7th Global Power, Energy and Communication Conference*, Bochum, Germany, Jul. 2025, pp. 953-959.

[30] T. Zang, Y. Xiao, Y. Liu *et al*., "Defense strategy against cyber attacks on substations considering attack resource uncertainty," *Journal of Modern Power Systems and Clean Energy*, vol. 13, no. 4, pp. 1335-1346, Jul. 2025.

[31] National Development and Reform Commission (NDRC). (2014, Dec.). Provisions on the security protection of electric power monitoring and control systems. [Online]. Available: https://www.gov.cn/gongbao/content/2014/content_2758709.htm

[32] A. Khan, M. Hosseinzadehtaher, M. B. Shadmand *et al*., "Cybersecurity analytics for virtual power plants," in *Proceedings of IEEE 12th International Conference on Power Electronics for Distributed Generation Systems*, Chicago, USA, Jul. 2021, pp. 1-5.

[33] J. Hu, Y. Zhang, Y. Cai *et al*., "Review and prospect on cyber security of virtual power plant," *Proceedings of the CSEE*, vol. 45, no. 8, pp. 2876-2899, Apr. 2025.

[34] Y. Gui, A. S. Siddiqui, S. M. Tamor *et al*., "Security vulnerabilities of smart meters in smart grid," in *Proceedings of 45th Annual Conference of the IEEE Industrial Electronics Society*, Lisbon, Portugal, 2019, pp. 3018-3023.

[35] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 1-33, Nov. 2011.

[36] P. L. Bhattar, N. M. Pindoriya, and A. Sharma, "Data manipulation attacks in electricity market with generative adversarial network for electric vehicle aggregator," in *Proceedings of IEEE 4th International Conference on Sustainable Energy and Future Electric transportation*, Hyderabad, India, Aug. 2024, pp. 1-5.

[37] Y. Li, N. Guo, L. Wang *et al*., "Distributed multi-scale attention and predictor-based control for AC microgrids with time delays and cyber failures," *Journal of Modern Power Systems and Clean Energy*, vol. 13, no. 5, pp. 1800-1812, Sept. 2025.

[38] W. Tang, Z. Zhang, and L. Xie, "Short interval replay attack detection for industrial cyber-physical systems based on wavelet coherence," in *Proceedings of IEEE 35th International Conference on Chinese Control and Decision Conference*, Yichang, China, May 2023, pp. 3082-3087.

[39] J. Sheng, "Research on SQL injection attack and defense technology of power dispatching data network: based on data mining," *Mobile Information Systems*, vol. 2022, no. 1, p. 6207275, Jul. 2022.

[40] B. A. Alohali and V. G. Vassialkis, "Secure and energy-efficient multicast routing in smart grids," in *Proceedings of IEEE 10th International Conference on Acoustics, Speech, and Signal Processing*, Singapore, Apr. 2015, pp. 1-6.

[41] S. Yang, K. Lao, H. Hui *et al*., "Secure frequency regulation in power system: a comprehensive defense strategy against FDI, DoS, and latency cyber-attacks," *Applied Energy*, vol. 379, pp. 124772, Feb. 2025.

[42] Y. Liu, M. Dong, K. Ota *et al*., "Activetrust: secure and trustable routing in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 2013-2027, Sept. 2016.

[43] D. I. Urbina, J. Giraldo, A. A. Cardenas *et al*., "Survey and new direc-

tions for physics-based attack detection in control systems," National Institute of Standard Technology, Tech. Rep. NIST GCR 16-010, Nov. 2016.
[44] S. Xu, Y. Xia, and H. Shen, "Analysis of malware-induced cyber attacks in cyber-physical power systems," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 12, pp. 3482-3486, Dec. 2020.
[45] R. Alajlan, M. M. H. Rahman, M. Al-Naeem *et al*., "A literature review on cybersecurity risks and challenges assessments in virtual power plants: current landscape and future research directions," *IEEE Access*, vol. 12, no.12, pp. 188813-188827, Dec. 2024.
[46] S. Agarwal and R. Sodhi, "A novel attack path detection framework considering cascading failures in an interdependent cyber-physical power system," *IEEE Transactions on Industrial Informatics*, vol. 21, no. 10, pp. 1-11, Jun. 2025.
[47] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan *et al*., "Cyber-physical power system (CPPS): a review on modeling, simulation, and analysis with cyber security applications," *IEEE Access*, vol. 8, no.8, pp. 151019-151064, Aug. 2020.
[48] K. Kang, N. Shi, K. Zhang *et al*., "A cloud-edge-end collaboration framework for fixed-time distributed optimization of virtual power plants," *Mathematics*, vol. 13, no. 11, p. 1883, Jun. 2025.
[49] M. I. El-Afifi, B. E. Sedhom, S. Padmanaban *et al*., "A review of IoT-enabled smart energy hub systems: rising, applications, challenges, and future prospects," *Renewable Energy Focus*, vol. 51, no.10, p. 100634, Oct. 2024.
[50] M. Raeispour, S. Yan, L. Meegahapola *et al*., "Cyber-physical security of virtual power plants: a survey," *IEEE Open Journal of the Industrial Electronics Society*, vol. 7, no. 4, pp. 416-441, Feb. 2026.
[51] K. Li, L. Qi, H. Zhang *et al*., "Cyber-physical coordinated attack path analysis considering attack preferences of cyber-physical power system," in *Proceedings of IEEE 5th International Conference on International Symposium on Computer Technology and Information Science*, Xi'an, China, May 2025, pp. 599-602.
[52] S. Wei, Z. Wu, J. Xu *et al*., "Security risk assessment and risk-oriented defense resource allocation for cyber-physical distribution networks against coordinated cyber attacks," *Journal of Modern Power Systems and Clean Energy*, vol. 13, no. 1, pp. 312-324, Jan. 2025.
[53] S. N. Islam, Z. Baig, and S. Zeadally, "Physical layer security for the smart grid: vulnerabilities, threats, and countermeasures," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6522-6530, Jul. 2019.
[54] N. Tatipatri and S. L. Arun, "A comprehensive review on cyber-attacks in power systems: impact analysis, detection, and cyber security," *IEEE Access*, vol. 12, no. 2, pp. 18147-18167, Feb. 2024.
[55] Y. Yang, Y. Zhou, J. Wu *et al*., "A failure tree model for cascading failure in power grid with uncertain renewable energy generation," *IEEE Transactions on Automation Science and Engineering*, vol. 22, no.6, pp. 4092-4108, Jun. 2024.
[56] Y. Zhang, L. Wang, W. Sun *et al*., "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 796-808, Dec. 2011.
[57] I. Semertzis, A. Ştefanov, A. Presekal *et al*., "Power system stability analysis from cyber attacks perspective," *IEEE Access*, vol. 12, no.8, pp. 113008-113035, Aug. 2024.
[58] W. N. Tayari, S. B. Elghali, E. H. Forushani *et al*., "Virtual power plants optimization issue: a comprehensive review on methods, solutions, and prospects," *Energies*, vol. 15, no. 10, p. 3607, May 2022.
[59] H. Gu, L. Zhao, Z. Han *et al*., "AI-enhanced cloud-edge-terminal collaborative network: survey, applications, and future directions," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 2, pp. 1322-1385, Dec. 2023.
[60] J. Stamp, A. McIntyre, and B. Ricardson, "Reliability impacts from cyber attack on electric power systems," in *Proceedings of 2009 IEEE/PES Power Systems Conference and Exposition*, Seattle, USA, Mar. 2009, pp. 1-8.
[61] D. Hou, Y. Sun, V. Dinavahi *et al*., "Adaptive two-stage unscented kalman filter for dynamic state estimation of synchronous generator under cyber attacks against measurements," *Journal of Modern Power Systems and Clean Energy*, vol. 12, no. 5, pp. 1408-1418, Sept. 2024.
[62] I. Makhdoom, M. Abolhasan, J. Lipman *et al*., "Anatomy of threats to the internet of things," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1636-1675, Oct. 2018.
[63] I. Semertzis, V. S. Rajkumar, A. Ştefanov *et al*., "Quantitative risk assessment of cyber attacks on cyber-physical systems using attack graphs," in *Proceedings of IEEE 10th* International *Conference on Workshop Modeling and Simulation of Cyber-physical Energy Systems*, Milan, Italy, May 2022, pp. 1-6.
[64] S. Chen, J. Xu, E. C. Sezer *et al*., "Non-control-data attacks are realistic threats," in *Proceedings of the 14th USENIX Security Symposium*, Baltimore, USA, Aug. 2005, p. 146.
[65] J. Zhang, Y. Zhang, G. Wang *et al*., "Vulnerability and resilience assessments of power grid based on community partition," *IEEE Transactions on Network Science and Engineering*, vol. 12, no. 4, pp. 3131-3144, Aug. 2025.
[66] R. Yang, H. Gao, F. Si *et al*., "Intelligent scene-adaptive desensitization: a machine learning approach for dynamic data privacy in virtual power plants," *Electronics*, vol. 13, no. 6, pp. 1051, Mar. 2024.
[67] H. Xing, G. Gong, M. Zhai *et al*., "Research on security and privacy protection of electric power data sharing," *Integrated Intelligent Energy*, vol. 46, no. 5, pp. 30-40, May 2024.
[68] Z. Chen, X. Chen, A. Ablaiti *et al*., "Analysis of intrusion detection method for power dispatching automation system based on deep reinforcement learning," *Electronic Technology*, vol. 54, no. 8, pp. 246-247, Aug. 2025.
[69] X. Shao, Z. Chen, B. Fu *et al*., "Leader-follower consensus-based privacy-preserving multi-objective dispatching for microgrid," in *Proceedings of IEEE 33rd International Conference on Chinese Control and Decision Conference*, Kunming, China, May 2021, pp. 4900-4905.
[70] C. Ni, L. Cang, P. Gope *et al*., "Data anonymization evaluation for big data and IoT environment," *Information Sciences*, vol. 605, no. C, pp. 381-392, May 2022.
[71] Q. Hu, S. Bu, W. Su *et al*., "A privacy-preserving energy management system based on homomorphic cryptosystem for IoT-enabled active distribution network," *Journal of Modern Power Systems and Clean Energy*, vol. 12, no. 1, pp. 167-178, Jan. 2024.
[72] D. Li, "Enterprise level network security: challenges and response strategies," *Digital Communications World*, vol. 9, no.9, pp. 197-199, Aug. 2024.
[73] J. Zuo, Q. Ai, D. Wang *et al*., "Privacy preserving trading strategy for power peak-shaving market with participation of virtual power plant," *Automation of Electric Power Systems*, vol. 48, no. 18, pp. 149-157, Sept. 2024.
[74] B. Liu, W. Li, X. Wang *et al*., "A power data privacy protection method based on secret sharing," in *Proceedings of 2024 IEEE 4th International Conference on Power, Electronics and Computer Applications*, Shenyang, China, Mar. 2024, pp. 1366-1370.
[75] W. Luan, P. Li, B. Zhao *et al*., "Optimization of internal transaction decisions in virtual power plant considering privacy protection," *Automation of Electric Power Systems*, vol. 48, no. 18, pp. 158-166, Sept. 2024.
[76] S. Aggarwal and N. Kumar, "Signature primitives," in *Advances in Computers*, vol. 121, Cambridge: Elsevier, 2021, pp. 109-121.
[77] C. Liu, S. Wang, Y. Zhao *et al*., "Review of the application of blockchain technology in virtual power plant transactions," *Electric Power Construction*, vol. 44, no. 4, pp. 130-144, Apr. 2023.
[78] J. W. Bos, W. Castryck, I. Iliashenko *et al*., "Privacy-friendly forecasting for the smart grid using homomorphic encryption and the group method of data handling," in *Proceedings of International Conference on Cryptology*, Dakar, Senegal, Apr. 2017, pp. 184-201.
[79] T. Yang, J. Zhang, S. Cai *et al*., "Collaborative scheduling method for multivirtual power plants considering privacy data protection," *Journal of Tianjin University (Science and Technology)*, vol. 57, no. 8, pp. 836-846, Aug. 2024.
[80] R. Wei, Y. Wang, X. Wang *et al*., "Federated learning based privacy-preserving renewable energy consumption for the local community," in *Proceedings of IEEE 5th International Conference on Power and Energy Technology*, Tianjin, China, Jul. 2023, pp. 1594-1599.
[81] Z. Dang, Y. Zhao, A. Xu *et al*., "Bidding method for virtual power plant operators considering privacy information protection," *Northeast Electric Power Technology*, vol. 44, no. 12, pp. 60-67, Oct. 2023.
[82] J. Heyden, N. Schlueter, P. Binfet *et al*., "Privacy-preserving power flow analysis via secure multi-party computation," *IEEE Transactions on Smart Grid*, vol. 16, no. 1, pp. 344-355, Sept. 2024.
[83] M. Huang, X. Cui, and Y. Wang, "Distributed differentially private energy management of virtual power plants," *Electric Power Systems Research*, vol. 234, p. 110687, Sept. 2024.
[84] R. Li, R. Onishi, and H. Yamana, "An implementation of private function evaluation using FHE and TEE for smart computing systems," in *Proceedings of IEEE International Conference on Premier Conference on Smart Computing*, Osaka, Japan, Jul. 2024, pp. 231-233.
[85] A. Al-Saedi, V. Boeva, and E. Casalicchio, "Reducing communication overhead of federated learning through clustering analysis," in *Proceedings of 2021 IEEE Symposium on Computers and Communica-*

tions, Athens, Greece, 2021, pp. 1-7.
[86] X. Wang, M. Yu, Y. Wang *et al*., "Attribute-based access control encryption," *IEEE Transactions on Dependable and Secure Computing*, vol. 22, no. 3, pp. 2227-2242, Jun. 2025.
[87] R. Yang, C. Shi, J. Fei *et al*., "Multi-scenarios in virtual plant with user attribute privacy protection using zero-knowledge proofs," *Electric Power Information and Communication Technology*, vol. 22, no. 9, pp. 33-44. Sept. 2024.
[88] S. Chen, J. Li, Y. Zhan *et al*., "Efficient revocable attribute-based encryption with verifiable data integrity," *IEEE Internet of Things Journal*, vol. 11, no. 6, pp. 10441-10451, Mar. 2024.
[89] D. Wang, Q. Ai, T. Yu *et al*., "Technical challenges and solutions for trusted trading of virtual power plant," *Automation of Electric Power Systems*, vol. 49, no. 19, pp. 8-25, Oct. 2025.
[90] A. Alagappan, S. K. Venkatachary, and L. J. B. Andrews, "Augmenting zero trust network architecture to enhance security in virtual power plants," *Energy Reports*, vol. 8, no. 11, pp. 1309-1320, Nov. 2022.
[91] M. Akhtar, A. Alharbi, and M. Tanveer, "Lightweight authentication framework for iot-centric smart healthcare systems," *Peer-to-Peer Networking and Applications*, vol. 19, no. 1, p. 28, Dec. 2025.
[92] A. M. A. D. Kaif, K. S. Alam, and S. K. Das, "Blockchain-based sustainable energy transition of a virtual power plant: conceptual framework design & experimental implementation," *Energy Reports*, vol. 11, no.6, pp. 261-275, Jun. 2024.
[93] Q. Wu and L. Hong, "Optimal scheduling research of virtual power plant based on blockchain," *Modern Industrial Economy and Informatization*, vol. 14, no. 10, pp. 209-211, Oct. 2024.
[94] S. Seven, G. Yao, A. Soran *et al*., "Peer-to-peer energy trading in virtual power plant based on blockchain smart contracts," *IEEE Access*, vol. 8, no. 8, pp. 175713-175726, Sept. 2020.
[95] S. Yu, Z. Wei, G. Sun *et al*., "A double auction mechanism for virtual power plants based on blockchain sharding consensus and privacy preservation," *Journal of Cleaner Production*, vol. 436, p. 140285, Jan. 2024.
[96] G. Justin and S. Paternain, "Graph neural networks for power system security assessment," in *Proceedings of IEEE 3rd International Conference on Power Systems and Electrical Technology*, Tokyo, Japan, Aug. 2024, pp. 882-886.
[97] P. Ananthi, K. N. Devi, D. Gopinath *et al*., "Enhancing cybersecurity in the supply chain through predictive analytics for cyber threats," in *Proceedings of IEEE 2nd International Conference on AI, Machine Learning and Applications*, Namakkal, India, Mar. 2024, pp. 1-5.
[98] S. Motupalli and S. Choi, "AI-driven security: investigating LLMs for automated vulnerability detection in code changes," in *Proceedings of International Conference on Silicon Valley Cybersecurity Conference*, San Francisco, USA, Jun. 2025, pp. 1-3.
[99] I. Erkek and E. Irmak, "Enhancing cybersecurity of a hydroelectric power plant using its digital twin model," in *Proceedings of IEEE 12th International Conference on Smart Grid*, Setubal, Portugal, May 2024, pp. 372-377.
[100] G. Sampedro, S. Ojo, M. Krichen *et al*., "Defending AI models against adversarial attacks in smart grids using deep learning," *IEEE Access*, vol. 12, pp. 157408-157417, Oct. 2024.
[101] A. Archa and K. Kartheeban, "Real time poisoning attacks and privacy strategies on machine learning systems," in *Proceedings of 2024 3rd International Conference on Sentiment Analysis and Deep Learning*, Bhimdatta, Nepal, Jul. 2024, pp. 183-189.
[102] S. Afrin, M. Muttaki, A. Anil *et al*., "AI-powered cybersecurity for smart grid communication: a systematic review of intrusion detection and threat mitigation systems," *Energy Conversion and Management: X*, vol. 29, no. C, p. 101416, Jan. 2026.
[103] M. Reis, "Lightweight signal processing and edge AI for real-time anomaly detection in IoT sensor networks," *Sensors*, vol. 25, no. 21, p. 6629, Oct. 2025.
[104] S. Haq, Y. Singh, A. Sharma *et al*., "A survey on IoT & embedded device firmware security: architecture, extraction techniques, and vulnerability analysis frameworks," *Discover Internet of Things*, vol. 3, no. 1, p. 17, Oct. 2023.

Jiayu Li received the M.S. degree from North China Electric Power University, Baoding, China, in 2021. He is currently working at Department of Electrical Engineering, Tsinghua University, Beijing, China. His research interests include virtual power plant and strategic energy planning.

Hongchao Gao received the Ph.D. degree from Chonnam National University, Gwangju, South Korea, in 2019. He worked with the Global Energy Research Institute of State Grid, Beijing, China, until 2019. He is currently an Assistant Researcher with State Key Laboratory of Power System Operation and Control, Department of Electrical Engineering, Tsinghua University, Beijing, China. His research interests include virtual power plant and microgrid.

Chongqing Kang received the Ph.D. degree from the Department of Electrical Engineering, Tsinghua University, Beijing, China, in 1997. He is currently a Professor with Tsinghua University, Beijing, China. His research interests include power system planning, power system operation, renewable energy, low-carbon electricity technology, and load forecasting.

Yiwei Cui is currently pursuing the M.Sc. degree at KTH Royal Institute of Technology, Stockholm, Sweden. He is currently a Research Intern with the Energy Internet Research Institute, Tsinghua University, Beijing, China. His research interests include virtual power plant and renewable energy techno-economics.

Wenmeng Zhao received the Ph.D. degree from South China University of Technology, Guangzhou, China, in 2016. He is currently working at Electric Power Research Institute, China Southern Power Grid, Guangzhou, China. His research interests include electricity market and optimal operation of power system.

Tian Mao received the Ph.D. degree from City University of Hong Kong, Hong Kong, China, in 2017. He is currently working at Electric Power Research Institute, China Southern Power Grid, Guangzhou, China. His research interests include virtual power plant and demand response.