Review

Federated Learning for Privacy-Preserving Defense in Power Cyber-Physical Systems: Frameworks, Techniques, and Challenges

Xiaokang Wang *

Posted Date: 2 June 2025

doi: 10.20944/preprints202506.0088.v1

Keywords: Power Cyber-Physical Systems; Federated Learning; Privacy-Preserving Defense; Cross-Layer Cybersecurity; Edge Computing; Collaborative Threat Detection

 doi:10.20944/preprints202506.0088.v1

Review

Federated Learning for Privacy-Preserving Defense in Power Cyber-Physical Systems: Frameworks, Techniques, and Challenges

Xiaokang Wang

School of Electrical Engineering, Guangxi University, Nanning, China; wang_xk525@outlook.com

Abstract: The increasing interconnection and digitalization of modern energy systems have intensified cybersecurity vulnerabilities in Power Cyber-Physical Systems (Power CPS). Traditional centralized defense approaches struggle to balance privacy preservation, scalability, and collaborative responsiveness across distributed infrastructures. Federated Learning (FL) emerges as a promising paradigm that enables distributed, privacy-preserving model training without sharing raw data. This review presents a comprehensive analysis of FL-based collaborative defense for Power CPS, spanning threat modeling, architectural taxonomies, privacy-preserving mechanisms, and real-world applications. We categorize FL techniques by learning structure, synchronization, and personalization, and examine privacy-enhancing technologies such as differential privacy, secure multiparty computation, homomorphic encryption, and trusted execution environments. Practical applications across substations, SCADA systems, WAMS, and EV infrastructures are reviewed alongside deployment challenges such as communication overhead, adversarial threats, and operational constraints. A roadmap is proposed for future research in cross-layer FL architectures, federated reinforcement learning, and regulatory standardization. The review concludes by advocating for cross-sector collaboration to operationalize federated defense as a cornerstone of resilient, secure, and privacy-compliant smart grids.

Keywords: power cyber-physical systems; federated learning; privacy-preserving defense; cross-layer cybersecurity; edge computing; collaborative threat detection

1. Introduction

1.1. Background on Cybersecurity in Power Cyber-Physical Systems

The global energy sector is undergoing a profound transformation driven by the convergence of physical grid operations with digital communication, control, and computation technologies, resulting in what is commonly known as Power Cyber-Physical Systems (Power CPS) [1-3]. These systems integrate components such as Supervisory Control and Data Acquisition (SCADA) systems [4], Distributed Energy Resources (DERs) [5-6], Advanced Metering Infrastructure (AMI), and Electric Vehicle (EV) charging networks [7-8], forming highly interconnected infrastructures that support the generation, transmission, distribution, and consumption of electricity [10-12].

While this integration enhances operational efficiency, situational awareness, and real-time control, it also introduces expanded cyber-attack surfaces. Malicious actors can exploit vulnerabilities in communication protocols, sensor networks, control algorithms, and data management platforms to disrupt grid operations, manipulate market mechanisms, or compromise customer data privacy [13-15]. Cyber-physical attacks such as False Data Injection Attacks (FDIAs), Denial-of-Service (DoS) attacks, ransomware campaigns, and insider threats have increasingly targeted energy infrastructures worldwide, threatening not only economic stability but also national security [16-18].

Traditional cybersecurity strategies in Power CPS rely heavily on centralized detection and defense mechanisms, where data is aggregated at control centers or cloud platforms for analysis and decision-making [19-20]. However, this centralized paradigm presents several limitations, including:

 doi:10.20944/preprints202506.0088.v1

- Data privacy concerns: Transferring sensitive operational data to central servers risks exposing confidential information [21].
- Scalability challenges: Centralized processing struggles to scale across geographically distributed and heterogeneous grid assets.
- Communication overhead: Continuous data transfer imposes significant bandwidth demands on grid communication networks.
- Delayed response times: Centralized analysis may be too slow to respond to rapidly evolving threats at the grid edge [22].

These challenges highlight the urgent need for decentralized, collaborative, and privacy-preserving defense frameworks that enable multiple stakeholders—such as utilities, DER operators, microgrid controllers, and EV aggregators—to cooperate in detecting and mitigating cyber threats without compromising data confidentiality or system performance [23].

1.2. The Need for Collaborative and Privacy-Preserving Defense Strategies

The highly distributed nature of Power CPS requires collaborative defense mechanisms that leverage local intelligence while maintaining global situational awareness [24]. For example, DER operators may detect localized anomalies that indicate a broader coordinated attack on the grid. Similarly, EV charging infrastructure operators may observe unusual behaviors that could signal ransomware propagation across control networks.

However, collaboration is hindered by data privacy regulations, competitive business interests, and technical barriers that prevent stakeholders from sharing raw operational data [25]. This tension creates a paradox: effective cyber defense requires information sharing, but information sharing risks exposing sensitive data [26-27].

Overcoming this paradox demands privacy-preserving collaborative defense frameworks that enable:

- Joint learning from distributed data sources without centralizing raw data.
- Cross-entity threat intelligence sharing without violating privacy or confidentiality constraints.
- Scalable and adaptive defense mechanisms that operate across diverse and distributed grid environments.

1.3. Emergence of Federated Learning as a Distributed Defense Paradigm

Federated Learning (FL) has emerged as a promising solution to this challenge. Originally proposed by Google for privacy-preserving mobile device learning, FL enables multiple entities to collaboratively train machine learning models without sharing raw data. Instead, participants perform local model training on their private data and share only model updates (e.g., gradients or weights) with a central aggregator, which combines them to produce a global model [28-30].

This decentralized learning paradigm offers several advantages for Power CPS cybersecurity:

- Privacy Preservation: Raw data remains local, reducing the risk of data leakage or regulatory non-compliance.
- Scalability: FL naturally scales to large, geographically distributed networks of grid assets.
- Low Communication Overhead: Only model updates, not raw data, are transmitted, reducing bandwidth requirements.

 doi:10.20944/preprints202506.0088.v1

- Collaboration Across Trust Boundaries: FL enables stakeholders with varying levels of trust to jointly improve defense capabilities.

In recent years, researchers have begun exploring the application of FL to various cybersecurity tasks in Power CPS, including:

- Anomaly and intrusion detection in substations, microgrids, and EV charging stations [31-33].
- Malware and ransomware detection in SCADA and Industrial Control Systems (ICS) [34].
- FDIA detection in wide-area monitoring and control systems [35-36].

While these early studies demonstrate the potential of FL, significant technical, operational, and organizational challenges remain in adapting FL to the unique requirements of Power CPS environments.

1.4. Objectives, Scope, and Structure of the Review

This review aims to offer a comprehensive, structured, and forward-looking analysis of FL and privacy-preserving collaborative defense in Power CPS. Specifically, it seeks to: characterize the cybersecurity challenges driving the need for decentralized and privacy-aware defense mechanisms; elucidate the principles of FL and its suitability for power system applications; survey and classify relevant FL methodologies; analyze privacy-preserving techniques such as differential privacy, secure multiparty computation, and trusted execution environments; review state-of-the-art applications of FL in Power CPS security; identify deployment bottlenecks and performance trade-offs; and propose research pathways to operationalize scalable and resilient federated defense.

The remainder of this review is structured as follows. Section 2 analyzes the evolving threat landscape and cyber-physical defense challenges. Section 3 introduces the foundational concepts of FL and its relevance to Power CPS. Section 4 categorizes existing FL architectures and algorithms for grid security. Section 5 explores privacy-preserving techniques integrated with FL. Section 6 surveys practical applications of FL in power grid cybersecurity. Section 7 discusses system deployment issues and evaluation metrics. Section 8 presents testbeds and validation use cases. Section 9 outlines future research priorities and collaborative development strategies. Finally, Section 10 concludes the review with strategic insights.

2. Threat Landscape and Defense Challenges in Power CPS

As modern power grids evolve into highly interconnected Power CPS, the attack surfaces they present to malicious actors have expanded dramatically. Adversaries increasingly exploit these expanded surfaces using multi-vector, cross-layer, and stealthy cyber-physical attacks [37]. These attacks target not just cyber infrastructure but also physical assets, market operations, and human operators, presenting unique defense challenges that traditional security architectures struggle to address [38-39].

This section reviews the emerging cyber-physical threat landscape in Power CPS and analyzes the technical and organizational barriers to achieving scalable, collaborative, and privacy-preserving defense.

2.1. Overview of Cyber-Physical Attacks on Power CPS

FDIAs represent one of the most well-documented and impactful types of cyber-physical threats to Power CPS. These attacks manipulate measurement data—originating from devices like Phasor Measurement Units (PMUs), Remote Terminal Units (RTUs), or smart meters—to deceive state estimation processes, initiate inappropriate control actions, or obscure actual system faults. Their

 doi:10.20944/preprints202506.0088.v1

effectiveness is largely due to the deep reliance of grid operations on data accuracy and the absence of robust cross-validation or authentication mechanisms [40-41]. In parallel, ransomware and malware attacks have gained prominence, with notable real-world incidents underscoring their disruptive potential. Such attacks encrypt operational data, block access to critical control interfaces, and spread across Information Technology (IT) and Operational Technology (OT) domains, paralyzing essential services [42-44].

Supply chain attacks and insider threats further exacerbate the vulnerability landscape. These threats introduce malicious software or leverage internal access to leak sensitive data, subvert policies, or grant unauthorized system access—undermining trust in even well-secured infrastructures [45]. Distributed Denial-of-Service (DDoS) attacks, meanwhile, aim to incapacitate communication infrastructure, effectively severing the links between field devices and control centers [46-47]. These disruptions delay critical decision-making and response activities. Finally, the emergence of coordinated multi-agent attacks, involving simultaneous actions across cyber, physical, and market layers, highlights the need for defenses that move beyond single-point, reactive strategies [48-49].

2.2. Challenges of Centralized Defense in Power CPS

Centralized defense architectures face inherent limitations in the context of Power CPS. A major obstacle is the issue of data privacy and ownership, as utilities and other stakeholders—including TSOs, DSOs, DER owners, and aggregators—are often bound by strict regulatory requirements and mutual distrust that inhibit operational data sharing [50-51]. This lack of transparency hinders collective threat visibility and coordinated response.

In addition, the sheer scale and heterogeneity of grid infrastructures strain centralized systems [52]. These platforms often lack the scalability to manage geographically distributed assets and fail to accommodate the diverse computational profiles of legacy and modern devices. Compounding this are communication bottlenecks in bandwidth-constrained environments, such as rural grids or isolated microgrids, where transmitting high-resolution data to centralized servers is neither timely nor feasible [53-54]. Furthermore, centralized systems introduce latency and single points of failure that can delay detection, response, and mitigation—making them inadequate for countering the fast-paced dynamics of cyber-physical threats [55].

2.3. The Role of Multi-Stakeholder Collaboration

Collaborative defense frameworks are essential for protecting complex and interdependent Power CPS ecosystems. These frameworks must facilitate real-time information exchange, distributed sensing, and synchronized control across diverse stakeholders. By pooling situational awareness and threat intelligence, collaborative mechanisms can detect broader attack patterns and respond more swiftly than isolated entities [56-58].

However, several barriers impede effective collaboration. Trust deficits between stakeholders—often arising from competition or differing priorities—hinder open communication [59]. Regulatory restrictions further limit data sharing, while the absence of standardized, privacy-preserving coordination technologies restricts the operational feasibility of collaborative models. Addressing these challenges requires the development of technical, legal, and institutional mechanisms that preserve security without compromising organizational autonomy [60].

2.4. Limitations of Existing Privacy-Preserving Methods

Although privacy-preserving techniques are increasingly employed in power system security, they come with significant limitations. Data anonymization methods, while simple to implement, often reduce data utility and are vulnerable to re-identification attacks using auxiliary information. Trusted third-party solutions, which centralize sensitive data for analysis, introduce new points of

 doi:10.20944/preprints202506.0088.v1

failure and require implicit confidence in external security practices—an assumption that does not always hold [61-63].

More advanced encryption-based techniques, such as homomorphic encryption, offer strong privacy guarantees but at the cost of high computational overhead, making them impractical for time-sensitive grid applications. These limitations underscore the need for innovative privacy-preserving approaches—such as federated learning—that can support distributed collaboration while maintaining robust data protection and system responsiveness [64-65].

2.5. Summary of Threats and Defense Challenges

To clarify the foundational motivations for adopting federated learning in Power CPS, Table 1 outlines key categories of cybersecurity challenges, emphasizing the technical and organizational limitations of centralized defenses and existing privacy-preserving approaches.

Table 1. Challenge Categories and Key issues in Power CPS.

Challenge Category	Key Issues
Cyber-Physical Threats	FDIAs, ransomware, insider threats, DDoS, coordinated multi-agent attacks
Centralized Defense Limits	Data privacy concerns, scalability, communication bottlenecks, delayed response
Collaboration Barriers	Trust deficits, regulatory constraints, lack of privacy-preserving frameworks
Privacy-Preserving Limits	Data utility loss, third-party reliance, computational overhead

In summary, the evolving cyber-physical threat landscape demands scalable, decentralized, and privacy-preserving defense strategies that overcome the limitations of centralized architectures. FL offers a promising pathway to achieve these objectives, as discussed in the next section.

3. Fundamentals of Federated Learning and Its Relevance to Power CPS

The emerging demands for collaborative, privacy-preserving, and distributed cyber defense in Power CPS have directed attention toward FL as a viable solution. Unlike traditional centralized machine learning, which requires collecting and storing data in a central repository, FL allows multiple parties to collaboratively train machine learning models without exposing their raw data [66-68].

This section introduces the principles, architectural components, operational workflow, and comparative advantages of Federated Learning, while explaining its unique suitability for Power CPS cybersecurity applications.

3.1. Principles of Federated Learning

FL is a decentralized machine learning paradigm in which multiple distributed clients collaboratively train a shared global model without exchanging raw data [69-71]. The core idea is to keep data localized on devices—such as substations, DER controllers, or smart meters—while sharing only model updates (e.g., gradients or weights) with a central server or aggregator [72-73]. The FL workflow typically involves the following steps: model initialization at the central server; local training by clients on their private data; submission of model updates to the aggregator; global model aggregation (often via weighted averaging); and redistribution of the updated model for further rounds of local training [74]. This iterative loop continues until convergence, ensuring data privacy and regulatory compliance.

3.2. Key Components of Federated Learning Architectures

 doi:10.20944/preprints202506.0088.v1

FL architectures consist of several critical components that enable collaborative learning while protecting data privacy [75]. Clients are entities that own local datasets and perform model training using their computational resources—these can range from edge devices in substations to smart inverters. The central aggregator coordinates the entire process, collects model updates, and computes the global model. Local models reside with each client and evolve through on-device training. The global model represents the shared knowledge built across all clients [76-77]. Secure communication protocols link clients to the aggregator, ensuring integrity and confidentiality during update exchanges. This modular architecture facilitates scalable and privacy-conscious collaboration in Power CPS.

The effective deployment of federated learning in Power Cyber-Physical Systems relies on a well-orchestrated interaction among several core components, each fulfilling a distinct role within the distributed learning architecture, as summarized in Table 2.

Table 2. Key Components and Their Roles in Federated Learning for Power CPS.

Component	Role in Federated Learning
Clients (Participants)	Entities with local datasets and computing resources (e.g., substations, DER operators)
Central Aggregator	Coordinates model aggregation and redistribution (can be centralized or decentralized)
Local Models	Machine learning models trained on client-specific data
Global Model	Aggregated model shared among all participants
Communication Protocol	Mechanism for securely exchanging model updates between clients and aggregator

3.3. Comparison with Centralized and Distributed Learning Approaches

Compared to traditional centralized learning, where all data is aggregated at a central location, FL offers significantly higher privacy by avoiding raw data transfer [78]. While distributed learning also decentralizes computation, it often involves some level of data sharing across nodes. FL improves on both fronts by limiting data movement to model updates, enabling high privacy, scalability, and reduced communication overhead. Centralized learning, although simple, suffers from privacy risks and bottlenecks. In contrast, FL is particularly well-suited for geographically dispersed, privacy-sensitive environments like Power CPS [79-81].

To contextualize the benefits of federated learning in Power CPS, Table 3 compares it with traditional centralized and distributed learning paradigms across key dimensions including data movement, privacy, scalability, and communication overhead.

Table 3. Comparative Analysis of Learning Paradigms for Power CPS Defense.

Learning Paradigm	Data Movement	Privacy Level	Scalability	Communication Overhead
Centralized Learning	Data collected centrally	Low (all data exposed)	Low (single bottleneck)	High (requires full data transfer)
Distributed Learning	Data partitioned and shared	Medium (partial data exposed)	Medium	Medium
Federated Learning	No raw data sharing, only models	High (data stays local)	High (scales across distributed clients)	Low (only model updates exchanged)

 doi:10.20944/preprints202506.0088.v1

3.4. Why Federated Learning Fits Power CPS

FL aligns naturally with the structure and constraints of Power CPS. First, it supports data locality and privacy preservation, allowing entities such as utilities and aggregators to retain control over sensitive data while contributing to global models. Second, FL is highly scalable, making it suitable for applications across extensive infrastructures like Wide-Area Monitoring Systems (WAMS), AMI, and EV charging networks [82]. Third, its low communication overhead is advantageous in bandwidth-constrained environments [83-84]. Furthermore, FL enables cross-organizational collaboration without requiring full trust between participants, thus fostering secure cooperation between TSOs, DSOs, and third-party vendors. Lastly, FL accommodates the computational diversity of the grid by supporting both high-capability edge devices and lightweight implementations for legacy systems [86].

To highlight the practical benefits of applying federated learning in power system cybersecurity, Table 4 summarizes the core technical and operational advantages that make FL particularly suitable for modern grid environments.

Table 4. Key Advantages of Federated Learning in Power CPS Security.

Advantage	Description
Privacy Preservation	Data remains local, reducing privacy risks and regulatory exposure
Scalability	Supports distributed, large-scale grid infrastructures
Communication Efficiency	Minimizes bandwidth consumption by transmitting only model updates
Cross-Entity Collaboration	Enables joint defense across organizational boundaries without raw data sharing
Heterogeneity Support	Adapts to diverse device capabilities, from edge to legacy systems

In summary, Federated Learning offers a compelling foundation for building privacy-preserving collaborative defense frameworks in Power CPS. The next section will introduce a detailed taxonomy of FL techniques and how they apply to various grid security scenarios.

4. Taxonomy of Federated Learning for Power CPS

FL architectures can be classified based on the distribution of features and samples across participating clients [87-89]. Horizontal Federated Learning (HFL) is used when clients have similar feature spaces but different datasets, such as substations with the same sensors deployed in distinct regions. This structure supports collaborative intrusion and anomaly detection in dispersed systems [90]. Vertical Federated Learning (VFL) applies when clients observe the same events but with different features, such as utility companies and market operators monitoring grid conditions from distinct perspectives [91]. VFL enables cross-domain detection strategies that blend operational and market insights. Federated Transfer Learning (FTL) addresses scenarios with both different feature and sample spaces, applying transfer learning to harmonize disparate data modalities—ideal for bridging modern and legacy infrastructure [92].

4.1. Categorization of FL Algorithms and Aggregation Methods

FL algorithms can be broadly categorized based on their aggregation strategies and optimization goals [93]. Federated Averaging (FedAvg) remains the most widely adopted method due to its simplicity and efficiency in averaging client updates. However, advanced variants—such as FedProx, FedNova, and Scaffold—address issues like client drift, data heterogeneity, and system imbalance [94-96]. Robust aggregation techniques like Krum, Trimmed Mean, and Bulyan further enhance resilience against poisoned or malicious clients, which is particularly important for adversarial

 doi:10.20944/preprints202506.0088.v1

settings in Power CPS [97]. Algorithm selection must consider convergence speed, communication efficiency, and robustness to non-iid data and client failures [98-100].

To clarify the application contexts of different federated learning paradigms, Table 5 classifies FL types based on their feature and sample space configurations, along with representative use cases in Power CPS.

Table 5. Classification of FL Types and Their Applications in Power CPS.

FL Type	Feature Space	Sample Space	Typical Application in Power CPS
Horizontal FL	Same	Different	Substation and microgrid intrusion detection
Vertical FL	Different	Same	Cyber-physical-market fraud detection
Transfer FL	Different	Different	Cross-utility, cross-technology defense

4.2. Synchronization Schemes in Federated Learning

Synchronization strategies in FL determine how client updates are coordinated [101-102]. Synchronous FL requires all clients to submit their updates in locked rounds, enabling consistent aggregation but suffering from straggler effects when slow clients delay the process [103]. It is well-suited for stable and coordinated environments. Asynchronous FL, by contrast, allows clients to update the global model independently, which reduces latency and accommodates network variability but may introduce stale updates and convergence instability [104-105]. This approach is advantageous for edge-based systems and heterogeneous Power CPS infrastructures where connectivity and compute capacity vary.

To highlight the impact of synchronization strategies on performance and applicability, Table 6 compares synchronous and asynchronous federated learning in terms of their advantages, challenges, and use cases in Power Cyber-Physical Systems.

Table 6. Comparison of Synchronous and Asynchronous FL in Power CPS.

Synchronization Type	Advantages	Challenges	Power CPS Use Cases
Synchronous FL	Predictable convergence, consistency	Straggler effect, communication bottlenecks	Coordinated substation-level defense
Asynchronous FL	Non-blocking updates, resilience to delays	Update staleness, convergence variance	Edge-based or DER-level collaborative defense

4.3. Personalization Techniques for Heterogeneous Power CPS Entities

Given the diversity of data and system characteristics across Power CPS, personalization in FL is essential [106-108]. Fine-tuning allows each client to adapt the global model to local data post-aggregation, enhancing relevance without disrupting shared learning. Clustered FL organizes clients into groups with similar distributions, enabling group-specific models that reflect regional or operational commonalities [109-110]. Meta-learning approaches build models that rapidly adapt to local conditions, improving generalization across diverse environments [111]. These techniques ensure that FL remains effective despite heterogeneity in grid assets, regions, and usage profiles.

4.4. FL-Enabled Collaborative Defense Frameworks

FL underpins a range of defense frameworks in Power CPS. For anomaly detection, it allows the fusion of diverse local patterns without exposing raw data, enhancing global threat awareness [112]. In attack classification, FL aggregates experiences across different environments, improving

 doi:10.20944/preprints202506.0088.v1

recognition of complex cyber-physical threats such as FDIAs or ransomware [113-115]. For distributed response coordination, FL facilitates real-time, privacy-respecting collaboration to identify compromised components and plan mitigation actions [116-118]. These frameworks illustrate the operational utility of FL as a foundation for mission-resilient, multi-agent grid security.

To provide a structured understanding of how various FL dimensions align with defense needs in Power CPS, Table 7 summarizes key aspects, corresponding techniques, and their typical application contexts.

Table 7. Overview of FL Dimensions and Their Applications in Power CPS.

Aspect	Categories/Techniques	Application Context
Learning Structure	Horizontal FL, Vertical FL, Federated Transfer Learning	Cross-entity, cross-domain, cross-technology defense
Synchronization Scheme	Synchronous FL, Asynchronous FL	Coordinated vs. distributed defense operations
Personalization Technique	Fine-tuning, clustered FL, meta-learning	Heterogeneous device and regional adaptation
Defense Application	Anomaly detection, attack classification, distributed response	Privacy-preserving collaborative defense across Power CPS

In summary, this taxonomy provides **a structured foundation** for selecting and adapting FL strategies to meet the **diverse and complex defense needs of Power CPS**. The next section will explore **privacy-preserving mechanisms** that further strengthen FL's security guarantees.

5. Privacy-Preserving Mechanisms in Federated Learning

While FL mitigates data privacy risks by retaining raw data on client devices, it does not inherently guarantee complete privacy [118-120]. Adversaries can exploit model update leakage, gradient inversion attacks, or model poisoning to infer sensitive information or compromise the collaborative training process [121-122]. Therefore, additional privacy-preserving mechanisms are essential to harden FL frameworks against inference threats and adversarial manipulations [123-125].

This section presents key privacy-preserving mechanisms that complement FL, including Differential Privacy (DP), Secure Multiparty Computation (SMC), Homomorphic Encryption (HE), and Trusted Execution Environments (TEE). It also discusses trade-offs between privacy, model accuracy, and computational overhead, providing guidance for Power CPS implementations.

5.1. Differential Privacy in Federated Learning

Differential Privacy (DP) ensures that the inclusion or exclusion of any single data record in a dataset has negligible impact on the model's output, thereby protecting individual data privacy [126-128]. In FL, DP is commonly implemented by adding calibrated random noise to model updates before they are sent to the aggregator and bounding the sensitivity of these updates [129].

The trade-off between privacy and utility is central to DP: stronger privacy requires more noise, which can degrade model accuracy [130-131]. In Power CPS, DP is particularly relevant for protecting customer data in AMI, securing operational patterns in DER systems, and ensuring compliance with privacy regulations such as GDPR and CCPA [132-134].

DP offers strong mathematical guarantees for protecting individual data contributions, making it particularly appealing for privacy-sensitive applications in FL [135-137]. Its implementation is relatively lightweight and straightforward, which facilitates integration into existing federated learning workflows. However, its effectiveness depends heavily on the careful tuning of privacy parameters, as excessive noise introduced for stronger privacy can significantly compromise model

 doi:10.20944/preprints202506.0088.v1

accuracy [138-149]. Thus, achieving an optimal balance between privacy protection and model utility remains a key challenge in practical deployments [140].

5.2. Secure Multiparty Computation

Secure Multiparty Computation (SMC) enables multiple entities to jointly compute a function over their inputs without revealing them to one another [141-142]. In FL, SMC is used to perform secure model aggregation, ensuring no party—including the aggregator—can access individual model updates [143].

Typical SMC protocols include secret sharing and garbled circuits. For Power CPS, SMC facilitates trustless collaboration among stakeholders like grid operators and market participants, eliminating reliance on any single trusted aggregator [144-145]. SMC offers robust privacy protection in FL by enabling collaborative model aggregation without exposing individual updates, even when the aggregator is untrusted or compromised. This makes SMC particularly suitable for trustless, fully decentralized collaboration scenarios in Power CPS, such as joint operations among grid operators and market entities [146-148]. Despite its strong privacy guarantees, SMC often incurs significant computational and communication overhead, and its implementation can be complex, requiring specialized cryptographic protocols like secret sharing or garbled circuits [149].

5.3. Homomorphic Encryption

HE allows computations on encrypted data, enabling secure model aggregation in FL without decrypting client updates [150-152]. HE can be partially (PHE) or fully homomorphic (FHE), depending on whether it supports limited or arbitrary operations [153].

In Power CPS, HE offers a promising solution for securing grid operation data and facilitating FL in untrusted environments, such as outsourced or third-party computation platforms [154-155]. By enabling computations directly on encrypted data, HE ensures that sensitive information remains protected throughout the entire training process, eliminating the need to trust the central aggregation server [156]. However, despite its strong privacy guarantees, HE—particularly in its fully homomorphic form—incurs substantial computational overhead and often struggles to meet the performance demands of latency-sensitive power system applications [157].

5.4. Trusted Execution Environments

TEEs provide hardware-based isolation for securely executing sensitive computations, making them a valuable asset in FL applications within Power CPS [158-160]. TEEs, such as Intel SGX and ARM TrustZone, enable confidential model aggregation on untrusted servers and protect local training processes on edge devices by enforcing execution integrity and data confidentiality at the hardware level. This approach offers strong security assurances with relatively low computational overhead compared to cryptographic methods like homomorphic encryption [161]. Nonetheless, TEEs are not without limitations; they are susceptible to side-channel attacks due to implementation vulnerabilities and often face constraints in memory capacity and scalability, which may hinder their effectiveness in large-scale, real-time grid applications [162-163].

5.5. Trade-offs and Design Considerations for Power CPS

Balancing privacy and utility is crucial. Overly aggressive privacy protection may reduce model performance or increase latency [164-165]. Lightweight mechanisms like DP are ideal for resource-constrained devices, whereas HE and SMC are suitable for high-assurance use cases with ample resources [166].

Deployment feasibility also depends on compatibility with legacy systems and real-time operational requirements. Privacy-preserving mechanisms must align with existing protocols (e.g., IEC 62351) to ensure seamless integration [167].

 doi:10.20944/preprints202506.0088.v1

Table 7 provides a comparative overview of key privacy-preserving mechanisms integrated with Federated Learning, evaluating their privacy strength, computational demands, and relevance to Power CPS applications.

Table 7. Comparative Analysis of Privacy-Preserving Mechanisms for FL in Power CPS.

Mechanism	Privacy Strength	Computational Overhead	Applicability to Power CPS
Differential Privacy	High (with tuned parameters)	Low to Medium	Customer data protection in AMI and DERs
Secure Multiparty Computation	Very High	High	Trustless collaboration across operators
Homomorphic Encryption	Very High	Very High (especially FHE)	High-assurance, privacy-critical operations
Trusted Execution Environments	High (hardware-dependent)	Low to Medium	Secure local and edge computations

In summary, integrating these **privacy-preserving mechanisms** with FL can significantly **enhance trustworthiness and security** in Power CPS collaborative defense frameworks. The next section will review **practical applications** of FL in real-world Power CPS cybersecurity scenarios.

6. Federated Learning Applications in Power CPS Security

Building upon the architectural and privacy foundations presented earlier, this section explores practical applications of FL in real-world Power CPS cybersecurity scenarios. These applications address critical domains such as anomaly detection in substations and microgrids, malware and ransomware mitigation in control systems, FDIA detection in WAMS, and security enhancement for EV charging infrastructure.

6.1. Anomaly and Intrusion Detection in Distributed Substations and Microgrids

In geographically distributed substations and microgrids, localized cyber-physical threats often go undetected due to operational silos [168]. Federated Learning offers a solution by allowing these entities to independently train intrusion detection models on their local datasets, which are then aggregated to form a comprehensive global model [169-171]. This decentralized approach enhances detection coverage, preserves operational privacy, and supports scalable defense without requiring raw data sharing [172]. A notable application involves using FL-based anomaly detectors trained on network flow data to collaboratively identify unauthorized Modbus TCP traffic across substations.

6.2. Malware and Ransomware Detection in Control Systems

SCADA and Industrial Control Systems (ICS) are prime targets for ransomware and malware. These threats manifest in control logs, network activity, and system calls, which are often proprietary and sensitive [173]. FL enables SCADA/ICS operators to collaboratively train behavioral detection models without revealing internal process logic or configurations [173-175]. This collective intelligence accelerates the identification of novel malware variants. One case example is the federated training of RNN-based models across grid operators to detect ransomware execution patterns in Programmable Logic Controller (PLC) logs [176].

6.3. FDIA Detection in Wide-Area Monitoring Systems

Cyber-attacks, like FDIAs, pose a major risk to WAMS by tampering with PMU data, thereby misleading state estimators and jeopardizing grid stability [177]. Through FL, Transmission and

 doi:10.20944/preprints202506.0088.v1

Distribution System Operators can collaboratively develop robust FDIA detection models, drawing on their respective regional data. The fusion of these localized insights enhances model generalization and improves situational awareness [178-179]. An example involves the use of federated GNNs to identify spatial-temporal anomalies in synchronized PMU data [180].

6.4. Federated Defense in EV Charging Infrastructure and V2G Systems

The proliferation of EV charging infrastructure and bidirectional Vehicle-to-Grid (V2G) systems introduces new security challenges, including protocol exploitation and unauthorized energy flows [181-183]. FL enables charging station operators and V2G aggregators to jointly train security models that detect anomalous behaviors while safeguarding customer data [184]. Such models can flag attacks targeting Open Charge Point Protocols (OCPP), identify unusual charging session dynamics, or monitor suspicious V2G operations. A compelling use case is the deployment of federated autoencoder-based anomaly detectors across service providers for real-time EV charging session monitoring [185-187].

To highlight the practical utility of Federated Learning in enhancing cybersecurity across critical components of Power Cyber-Physical Systems, Table 8 summarizes representative application areas, associated threats, and the specific advantages FL provides.

Table 8. Applications of Federated Learning for Cybersecurity in Power CPS.

Application Area	Threat Addressed	FL Advantage
Substations and Microgrids	Unauthorized access, sensor tampering	Distributed anomaly detection without data centralization
SCADA/ICS Systems	Malware, ransomware	Collective behavioral malware detection
WAMS and PMU Networks	False data injection attacks	Cross-regional FDIA detection leveraging local data
EV Charging and V2G Systems	Protocol exploitation, grid injection manipulation	Scalable defense across charging infrastructure

In summary, FL enables a new class of collaborative, privacy-preserving, and scalable defense solutions for diverse Power CPS cybersecurity applications. The next section will discuss the practical challenges and performance trade-offs encountered when deploying FL in operational grid environments.

7. Practical Deployment Challenges and Performance Considerations

While FL presents a promising paradigm for collaborative, privacy-preserving defense in Power CPS, its real-world deployment poses several technical and operational challenges. These include communication overhead, convergence difficulties with heterogeneous data, security vulnerabilities within the FL process itself, and resource limitations across diverse grid infrastructures [188-190].

7.1. Communication Efficiency and Bandwidth Limitations

7.1.1. Communication Overhead in FL

Communication in FL is more efficient than traditional centralized learning, yet it is not trivial [191]. The volume of transmitted model updates can still strain network capacity—especially in bandwidth-constrained settings typical of distributed power systems. Factors contributing to communication load include model complexity, the frequency of update synchronization, and the number of participating devices [192]. To mitigate this, techniques such as model compression (e.g.,

 doi:10.20944/preprints202506.0088.v1

quantization, pruning), reduced update frequency via asynchronous FL, and hierarchical FL structures (e.g., regional aggregators) can significantly improve scalability [193-195].

7.2. Model Convergence, Drift, and Personalization

Convergence in FL becomes problematic with non-IID data, leading to slow training, unstable models, or bias toward dominant clients. Furthermore, temporal changes in local data—such as seasonality in energy demand—may cause model drift [196]. Effective personalization strategies such as local fine-tuning, clustered FL, and meta-learning can improve adaptability and robustness. These approaches tailor the global model to local operating contexts without sacrificing collaborative learning benefits [197].

7.3. Adversarial Attacks on Federated Learning

FL itself can be a target of attacks. Model poisoning occurs when malicious clients send corrupted updates to compromise the global model or insert backdoors [198]. Inference attacks—such as gradient inversion—threaten data confidentiality. Defense mechanisms include Byzantine-robust aggregation techniques (e.g., Krum, Median), differential privacy to obfuscate update content, and secure aggregation protocols that prevent exposure of individual updates. These measures are critical for ensuring trust and resilience in collaborative grid defense [199-200].

7.4. Resource Constraints in Edge and Legacy Devices

The heterogeneity of grid assets introduces disparities in computational capacity [201]. Legacy or embedded devices may lack sufficient memory, processing power, or energy to participate fully in FL. Deployment feasibility can be improved through lightweight model architectures (e.g., MobileNet), collaborative computing between edge nodes and the cloud, and selective participation schemes that allocate tasks to capable nodes while preserving overall system coverage [202-203].

7.5. Organizational and Operational Challenges

Beyond technology, deploying FL at scale in Power CPS requires addressing organizational complexities. Cross-stakeholder coordination is often hampered by trust deficits, incompatible policies, and unclear incentives. Establishing transparent governance, aligned data policies, and mutual benefits is essential for sustainable collaboration [204]. Moreover, FL integration must be seamless with existing grid management systems (e.g., SCADA, EMS, DERMS), and should minimize disruption to critical real-time operations during testing and rollout phases [205-206].

To ensure the successful deployment of Federated Learning in Power CPS environments, it is essential to address several technical and organizational challenges. Table 9 outlines key issues along with corresponding mitigation strategies.

Table 9. Deployment Challenges and Mitigation Strategies for Federated Learning in Power CPS.

Challenge	Key Issues	Mitigation Strategies
Communication Efficiency	High model update size and frequency	Model compression, asynchronous updates, hierarchical FL
Model Convergence and Drift	Non-IID data, model instability, distribution changes	Fine-tuning, clustered FL, meta-learning
Adversarial Threats to FL	Model poisoning, inference attacks	Byzantine-robust aggregation, differential privacy, secure aggregation
Resource Constraints	Limited computation, memory, energy	Lightweight models, edge-cloud collaboration, selective participation

 doi:10.20944/preprints202506.0088.v1

Challenge	Key Issues	Mitigation Strategies
Organizational and Operational	Trust barriers, policy misalignment, integration difficulties	Cross-stakeholder agreements, legacy system compatibility

While FL presents significant potential for enhancing privacy-preserving collaborative defense, its successful deployment requires careful management of technical, organizational, and operational trade-offs [207]. The next section will review validation platforms, testbeds, and case studies to demonstrate how these challenges are being addressed in practice.

8. Validation, Testbeds, and Real-World Case Studies

Although FL for Power CPS cybersecurity is gaining increasing academic attention, its practical validation is essential for demonstrating feasibility, quantifying performance, and fostering stakeholder confidence [208-210]. Validation efforts have centered around the use of digital twins and co-simulation frameworks, purpose-built testbeds, and real-world pilot deployments.

8.1. Digital Twin and Co-Simulation-Based Validation

8.1.1. Concept of Digital Twins for Power CPS

Digital twins serve as high-fidelity virtual counterparts to physical power systems, replicating operational behavior in real or near-real time [211-213]. These systems integrate grid simulators such as DIgSILENT PowerFactory and PSCAD, network emulators like Mininet or ns-3, control platforms such as MATLAB/Simulink, and energy market simulators like PLEXOS. When coupled with federated learning, digital twins facilitate holistic evaluation of FL-enabled defense mechanisms under realistic operational scenarios. Co-simulation frameworks, which interconnect these simulation domains, support the multi-layer testing of attack detection strategies, defense effectiveness, and the impact of FL on overall system stability and market performance [214-215]. Representative validation scenarios include FL-based FDIA detection across wide-area PMU networks and anomaly identification in simulated EV charging stations, capturing spatiotemporal variability and adversarial behavior [216].

8.2. FL Testbed Architectures for Power CPS Security

Complementing simulation-based approaches, dedicated testbeds have been developed to support experimental research on FL in cyber-physical energy systems [217]. These testbeds typically consist of distributed data sources (real or synthetic), edge computing nodes with localized training capabilities, hierarchical model aggregators, adversarial emulators to simulate attacks, and performance monitoring units [218]. For instance, national laboratory infrastructures integrate power grid emulators with cybersecurity toolkits to conduct realistic attack-defense experiments. Other testbeds adapt existing IoT FL environments to the specific constraints of grid edge devices, focusing on bandwidth limitations and heterogeneous computation. Academic-industry collaborations have also produced test environments for validating FL-based control and monitoring strategies in distributed energy resource management systems (DERMS) [219-220].

8.3. Performance Benchmarking and Metrics

8.3.1. Key Evaluation Metrics

To objectively compare FL strategies, a diverse set of benchmarking metrics is employed. These encompass model accuracy (e.g., precision, recall, F1-score), communication efficiency (e.g., update size and frequency), computational resource usage, convergence behavior, and security/privacy guarantees such as resistance to inference or poisoning attacks [221-222]. In addition to these technical

 doi:10.20944/preprints202506.0088.v1

indicators, operational metrics—such as the impact on grid stability and latency in detection-response workflows—are gaining importance. Evaluation typically involves comparative analysis with centralized or local models, stress testing under simulated attack conditions, and scalability assessments involving variable network and participant configurations [223-224].

Evaluating the effectiveness of Federated Learning in Power CPS requires a multidimensional set of metrics spanning model performance, system efficiency, and operational impact [225]. Table 10 presents representative metrics across key evaluation categories.

Table 10. Evaluation Metrics for FL in Power Cyber-Physical Systems.

Metric Category	Representative Metrics
Model Accuracy	Detection rate, precision, recall, F1-score
Communication Efficiency	Bandwidth consumption, update size, synchronization frequency
Computational Overhead	CPU usage, memory consumption, training time
Convergence Behavior	Number of rounds to convergence, model stability
Privacy and Security	Resistance to inference and poisoning attacks, privacy loss bounds
Operational Impact	Effect on grid stability, latency in detection-to-response pipeline

8.4. Emerging Real-World Case Studies

Emerging case studies further underscore the viability of FL in real-world settings. In one example, regional transmission system operators (TSOs) in Europe jointly trained graph neural networks (GNNs) using FL on PMU data streams, successfully enhancing spatial-temporal FDIA detection while preserving data sovereignty and reducing cross-border communication overhead [226]. In another case, EV charging service providers across North America leveraged federated autoencoder models to detect unauthorized usage behaviors without revealing individual customer patterns, demonstrating scalability across widespread assets [227]. A third case involved an Asian utility consortium deploying FL-based recurrent neural networks (RNNs) for ransomware detection within SCADA environments, enabling proactive malware defense without sharing proprietary control logic [228].

Effective validation of Federated Learning approaches in Power CPS necessitates diverse tools and methodologies to ensure technical robustness and real-world applicability. Table 11 outlines key validation aspects and corresponding insights.

Table 11. Validation Tools and Insights for Federated Learning in Power CPS.

Validation Aspect	Key Insights
Digital Twin and Co-Simulation	Enables multi-domain, realistic validation of FL defenses
FL Testbed Architectures	Support end-to-end performance evaluation in controlled environments
Benchmarking Metrics	Provide comprehensive assessment of accuracy, efficiency, and resilience
Real-World Case Studies	Demonstrate feasibility, scalability, and privacy preservation in practice

In summary, existing validation efforts and case studies demonstrate that Federated Learning can be effectively adapted and deployed in diverse Power CPS cybersecurity scenarios, though further research and field-scale demonstrations are needed to achieve widespread adoption. The next section outlines these future research priorities and cross-sector collaboration pathways.

 doi:10.20944/preprints202506.0088.v1

9. Future Research Directions and Collaborative Roadmap

9.1. Cross-Layer Federated Defense Architectures

One critical direction is the advancement of cross-layer FL defense mechanisms that transcend the cyber layer to integrate insights and actions across the physical, market, and human decision layers [229-230]. Existing FL deployments typically isolate single domains, yet real-world attacks often exploit interdependencies. Future architectures should enable joint modeling and fusion of data across domains, allowing coordinated multi-layer responses that preserve scalability and privacy [231].

9.2. Federated Reinforcement Learning for Adaptive Cyber-Physical Security

Another imperative is to move beyond supervised learning by leveraging Federated Reinforcement Learning (FRL) to dynamically adapt to unknown threats [232]. FRL can learn optimal defense policies through interactive feedback with simulated or operational grid environments, enabling responsive and distributed decision-making under uncertainty [233]. This is especially valuable where labeled datasets are scarce or evolving.

9.3. Trustworthy and Robust FL under Adversarial Conditions

Robustness and trustworthiness also remain pressing concerns. Adversarial participants can compromise FL through model poisoning or inference attacks on shared updates [234]. Research must focus on resilient aggregation algorithms, advanced privacy-preserving methods like differential privacy and secure multiparty computation, and trust frameworks that formalize collaboration among heterogeneous stakeholders.

9.4. Scalable FL Architectures for Resource-Constrained Grid Devices

Moreover, to broaden FL adoption across the diverse landscape of grid assets, scalable and lightweight model architectures must be developed. Many edge devices in the power system are resource-constrained, with limited processing, memory, and energy capacity. Tailoring FL algorithms to such environments, supported by edge-cloud collaboration and selective participation strategies, is essential for practical deployment [235].

9.5. Policy, Regulation, and Standardization Support

Policy and regulatory advancements are also required. The absence of clear standards and compliance frameworks for FL in critical infrastructure poses barriers to implementation [236]. Engagement with standards bodies (e.g., IEEE, IEC) to define deployment protocols, privacy benchmarks, and certification mechanisms is vital. Regulatory sandbox environments can serve as innovation zones for safely testing FL deployments.

9.6. Cross-Sector and Global Collaboration Mechanisms

The success of FL in Power CPS hinges on cross-sector and international collaboration. Siloed development efforts limit generalizability and slow progress [237]. Establishing multi-stakeholder consortia involving utilities, vendors, academia, and regulators will enable broader knowledge sharing, method harmonization, and coordinated deployment. Global cooperation is key to aligning methodologies, fostering trust, and building resilient energy systems across borders [238].

To accelerate the operationalization of Federated Learning in Power CPS, future efforts must prioritize key technical, infrastructural, and collaborative actions. Table 12 summarizes strategic focus areas and recommended initiatives.

Table 12. Strategic Priorities and Key Actions for Advancing FL in Power CPS.

 doi:10.20944/preprints202506.0088.v1

Priority Area	Key Actions
Cross-Layer Federated Defense	Develop multi-domain FL models and defense coordination frameworks
Federated Reinforcement Learning	Enable adaptive, policy-driven cyber-physical defense mechanisms
FL Robustness and Trustworthiness	Strengthen aggregation, privacy, and trust models
Scalable FL for Edge Devices	Design lightweight models and edge-cloud architectures
Regulatory and Standardization Frameworks	Define deployment standards, privacy compliance, and certification
Cross-Sector and International Collaboration	Build consortia and promote global knowledge sharing

In summary, realizing the full potential of federated learning in Power CPS requires a coordinated research and collaboration effort spanning technical innovation, regulatory alignment, and cross-sector partnerships. The final section will synthesize these findings and present strategic recommendations for future action.

10. Conclusion

This review has synthesized the state of the art in federated learning for power cyber-physical systems security, presenting an in-depth analysis of FL architectures, privacy-preserving mechanisms, practical implementations, and validation strategies. It has demonstrated how FL enables distributed learning without compromising sensitive data, fostering collaborative intelligence across grid operators, edge devices, and utility infrastructures. The review also highlighted practical challenges such as communication overhead, model personalization, adversarial vulnerabilities, and resource constraints, providing strategies to mitigate these issues through hierarchical architectures, secure aggregation, and edge-cloud coordination.

Unlocking the full potential of federated learning in power cyber-physical systems hinges on the advancement of integrated cross-layer and reinforcement learning frameworks, the design of lightweight and resource-efficient models for deployment on constrained edge devices, and the development of secure, transparent, and trustworthy collaboration mechanisms across heterogeneous stakeholders. Equally important are policy efforts to establish regulatory standards, certification frameworks, and collaborative consortia to support safe and effective FL adoption. By combining technological advances with institutional support and international cooperation, federated learning can serve as a cornerstone for building secure, resilient, and privacy-preserving smart grids of the future.

References

1. Quan M K, Pathirana P N, Wijayasundara M, et al. Federated Learning for Cyber Physical Systems: A Comprehensive Survey[J]. IEEE Communications Surveys & Tutorials, 2025.
2. [2 Soomro I A, Hussain S J, Ashraf Z, et al. Lightweight privacy-preserving federated deep intrusion detection for industrial cyber-physical system[J]. Journal of Communications and Networks, 2024, 26(6): 632-649.
3. Qu Z, Zhao T, Zhang Y, et al. Determination Method of Network Risk Propagation Threshold in Power CPS Based on Percolation Theory[J]. Automation of Electric Power Systems, 2020, 44(4): 16-23.
4. Sanjab A, Saad W. Data Injection Attacks on Smart Grids With Multiple Adversaries: A Game-Theoretic Perspective[J]. IEEE Transactions on Smart Grid, 2016, 7(4): 2038-2049.
5. Li Y, Yang Z, et al. Optimal scheduling of an isolated microgrid with battery storage considering load and renewable generation uncertainties[J]. IEEE Transactions on Industrial Electronics, 2018, 66(2): 1565-1575.

 doi:10.20944/preprints202506.0088.v1

6. Qin B, Liu D. Research Progress and Prospects on Analysis and Control of Power Grid Cyber-Physical Systems[J]. Proceedings of the CSEE, 2020, 40(18): 5816-5826.
7. Bo X, Chen X, Li H, et al. Modeling Method for the Coupling Relations of Microgrid Cyber-Physical Systems Driven by Hybrid Spatiotemporal Events[J]. IEEE Access, 2021, 9: 19619-19631.
8. Shang Y, Li D, et al. Explainable spatiotemporal multi-task learning for electric vehicle charging demand prediction[J]. Applied Energy, 2025, 384: 125460.
9. Li Y, He S, Li Y, et al. Federated multiagent deep reinforcement learning approach via physics-informed reward for multimicrogrid energy management[J]. IEEE Transactions on Neural Networks and Learning Systems, 2024, 35(5): 5902 - 5914.
10. Abdelkader S, Amissah J, Abdel-Rahim O. Virtual power plants: an in-depth analysis of their advancements and importance as crucial players in modern power systems[J]. Energy, Sustainability and Society, 2024, 14(1): 52.
11. Cao J, Wang Q, Qu Z, et al. Method for identifying false data injection attacks in power grid based on improved CNN-LSTM[J]. Electrical Engineering, 2025: 1-26.
12. Hoenig A, Roy K, Acquaah Y T, et al. Explainable AI for cyber-physical systems: Issues and challenges[J]. IEEE access, 2024, 12: 73113-73140.
13. Zhao J, An K, Wang X. Research on Fast Early Warning of False Data Injection Attack in CPS of Electric Power Communication Network[J]. Journal of Cyber Security and Mobility, 2024: 1331–1356-1331–1356.
14. Jiang Y, Wu S, Ma R, et al. Monitoring and defense of industrial cyber-physical systems under typical attacks: From a systems and control perspective[J]. IEEE Transactions on Industrial Cyber-Physical Systems, 2023, 1: 192-207.
15. Li Y, Li Z, Chen L, et al. A false data injection attack method for generator dynamic state estimation[J]. Transactions of China Electrotechnical Society, 2019, 34: 3651-3660.
16. Qu Z, Dong Y, Qu N, et al. Quantitative Assessment of Survivability of Power CPS Considering Load Optimization and Reconfiguration[J]. Automation of Electric Power Systems, 2019, 43(6): 15-24.
17. Suprabhath Koduru S, Machina V S P, Madichetty S. Cyber attacks in cyber-physical microgrid systems: A comprehensive review[J]. Energies, 2023, 16(12): 4573.
18. Namakshenas D, Yazdinejad A, Dehghantanha A, et al. IP2FL: Interpretation-based privacy-preserving federated learning for industrial cyber-physical systems[J]. IEEE Transactions on Industrial Cyber-Physical Systems, 2024.
19. Wang L, Xu P, Qu Z, et al. Coordinated Cyber-Attack Detection Model of Cyber-Physical Power System Based on the Operating State Data Link[J]. Frontiers in Energy Research, 2021, 9: 666130.
20. Lin W T, Chen G, Zhou X. Privacy-preserving federated learning for detecting false data injection attacks on power system[J]. Electric Power Systems Research, 2024, 229: 110150.
21. Zhu H, Xu L, Bao Z, et al. Secure control against multiplicative and additive false data injection attacks[J]. IEEE Transactions on Industrial Cyber-Physical Systems, 2023, 1: 92-100.
22. Wang T, Sun C, Gu X, et al. Modeling of Power Communication Coupled Networks and Their Vulnerability Analysis[J]. Proceedings of the CSEE, 2018, 38(12): 3556-3567.
23. Sakhare N N, Kulkarni R, Rizvi N, et al. A Decentralized Approach to Threat Intelligence using Federated Learning in Privacy-Preserving Cyber Security[J]. Journal of Electrical Systems, 2023, 19(3).
24. Yao P, Yan B, Yang Q. Game Theoretical Decision-Making of Dynamic Defense in Cyber-Physical Power Systems under Cyber-Attacks[J]. ACM Transactions on Cyber-Physical Systems, 2025, 9(2): 1-21.
25. Karamdel S, Liang X, Faried S O, et al. Optimization models in cyber-physical power systems: A review[J]. IEEE Access, 2022, 10: 130469-130486.
26. Chen J, Zhu Q. A cross-layer design approach to strategic cyber defense and robust switching control of cyber-physical wind energy systems[J]. IEEE Transactions on Automation Science and Engineering, 2022, 20(1): 624-635.
27. Kausar F, Deo S, Hussain S, et al. Federated Deep Learning Model for False Data Injection Attack Detection in Cyber Physical Power Systems[J]. Energies, 2024, 17(21): 5337.
28. Wang W, Di Maio F, Zio E. Adversarial risk analysis to allocate optimal defense resources for protecting cyber–physical systems from cyber attacks[J]. Risk Analysis, 2019, 39(12): 2766-2785.

 doi:10.20944/preprints202506.0088.v1

29. Barboni A, Rezaee H, Boem F. Detection of Covert Cyber-Attacks in Interconnected Systems: A Distributed Model-Based Approach[J]. IEEE Transactions on Automatic Control, 2020, 65(9): 3728-3741.
30. Rahman S, Pal S, Jadidi Z, et al. Robust Cyber Threat Intelligence Sharing Using Federated Learning for Smart Grids[J]. IEEE Transactions on Computational Social Systems, 2025, 12(2): 635 - 644.
31. Li Y, He S, Li Y, et al. Probabilistic charging power forecast of EVCS: Reinforcement learning assisted deep learning approach[J]. IEEE Transactions on Intelligent Vehicles, 2022, 8(1): 344-357.
32. Wen C, Yang L. A review on defense strategies against cyber-physical system attacks[J]. Control Theory & Applications, 2024, 41(12):130-138.
33. Qu Z, Zhang Y, Qu N, et al. Method for Quantitative Estimation of the Risk Propagation Threshold in Electric Power CPS Based on Seepage Probability[J]. IEEE Access, 2018, 6: 68813-68823.
34. Suneetha B, Kesavan R. A Survey on Privacy-Preserving Communication Frameworks in Machine Learning for Cybersecurity Threat Detection[C]//2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS). IEEE, 2024: 1354-1359.
35. Fan X, Lin W, Liu Z, Zhao L. Reachable Set Control for Nonlinear Markov Jump Cyber-Physical Systems with False Data Injection Attacks[J]. Journal of The Franklin Institute, 2024, 361(1): 224-233.
36. Guo G, Qi X, Wang R, et al. Integrated demand response mechanism for integrated energy systems based on federated learning[J]. Electric Power Automation Equipment, 2023, 43(8):201-210.
37. Wang L, Qu Z, et al. Method for Extracting Patterns of Coordinated Network Attacks on Electric Power CPS Based on Temporal-Topological Correlation[J]. IEEE Access, 2020, 8: 57260-57272.
38. Ni M, Li M, Li J, et al. Concept and research framework for coordinated situation awareness and active defense of cyber-physical power systems against cyber-attacks[J]. Journal of Modern Power Systems and Clean Energy, 2020, 9(3): 477-484.
39. Wang Y, et al. Collaborative optimization of multi-microgrids system with shared energy storage based on multi-agent stochastic game and reinforcement learning[J]. Energy, 2023, 280: 128182.
40. Wang L, Qu Z, Li Y, et al. Method for Extracting Patterns of Coordinated Network Attacks on Electric Power CPS Based on Temporal–Topological Correlation[J]. IEEE Access, 2020, 8: 57260-57272.
41. Bo X, Qu Z, Liu Y, et al. Review of active defense methods against power cps false data injection attacks from the multiple spatiotemporal perspective[J]. Energy Reports, 2022, 8: 11235-11248.
42. Qu Z, Qu N, Zhou Y, et al. Extraction of Typical Operating Scenarios of New Power System Based on Deep Time Series Aggregation[J]. CAAI Transactions on Intelligence Technology, 2024, 1-17. DOI: 10.1049/cit2.12369.
43. Niu H, Jagannathan S. Optimal defense and control of dynamic systems modeled as cyber-physical systems[J]. The Journal of Defense Modeling and Simulation, 2015, 12(4): 423-438.
44. Chen L, Gu S, Wang Y, et al. Stacked Autoencoder Framework of False Data Injection Attack Detection in Smart Grid[J]. Mathematical Problems in Engineering, 2021, 2021(1): 2014345.
45. Li Y, Cao J, Xu Y, et al. Deep learning based on Transformer architecture for power system short-term voltage stability assessment with class imbalance[J]. Renewable and Sustainable Energy Reviews, 2024, 189: 113913.
46. Wang Q, Tai W, Tang Y, et al. A Review of False Data Injection Attack Research for Power Cyber-Physical Systems[J]. Acta Automatica Sinica, 2019, 45(1): 72-83.
47. Wang J, Li Y, Xu T. Modeling of False Data Injection Attacks and Rapid Screening of Vulnerable Lines under Attacks[J]. Electric Power Construction, 2022, 43(1): 104-112.
48. Qu Z, Dong Y, Qu N, et al. Survivability Evaluation Method for Cascading Failure of Electric Cyber Physical System Considering Load Optimal Allocation[J]. Mathematical Problems in Engineering, 2019, 2019: 2817586.
49. Zang T, Tong X, Li C, et al. Research and Prospect of Defense for Integrated Energy Cyber–Physical Systems Against Deliberate Attacks[J]. Energies, 2025, 18(6): 1479.
50. Li Y, Li J, Chen L. Dynamic state estimation of synchronous machines based on robust cubature Kalman filter under complex measurement noise conditions[J]. Transactions of china electrotechnical society, 2019, 34(17): 3651-60.

 doi:10.20944/preprints202506.0088.v1

51. Liao Y, Wang Y, Cui Q, et al. Data-Driven Cyber-Physical Anomaly Detection With GAN in Federated Smart Factories[J]. IEEE Transactions on Industrial Informatics, 2025, 21(4): 3067 - 3076.
52. Lydia M, Prem Kumar G E, Selvakumar A I. Securing the cyber-physical system: A review[J]. Cyber-Physical Systems, 2023, 9(3): 193-223.
53. Chen L, Jin P, Yang J, et al. Robust Kalman Filter-Based Dynamic State Estimation of Natural Gas Pipeline Networks[J]. Mathematical Problems in Engineering, 2021, 2021(1): 5590572.
54. Zhou Y, Xiao H, Pei W, et al. Collaborative optimization and policy evolution of microgrid clusters based on vertical federated learning[J]. Automation of Electric Power Systems, 2023, 47(11): 121–132.
55. Li B, Liu Y, Li H, et al. Reflections on power information system security from the Ukrainian blackout accident[J]. China Electric Power, 2017, 50(5): 71.
56. Chamana M, Bhatta R, Schmitt K, et al. An integrated testbed for power system cyber-physical operations training[J]. Applied Sciences, 2023, 13(16): 9451.
57. Wang J, Xu G, Lei W, et al. CPFL: An effective secure cognitive personalized federated learning mechanism for industry 4.0[J]. IEEE Transactions on Industrial Informatics, 2022, 18(10): 7186-7195.
58. Dorbala S Y, Bhadoria R S. Analysis for security attacks in cyber-physical systems[J]. Cyber-Physical Systems: A Computational Perspective, 2015: 395-414.
59. Hu S, Yu S, Li H, et al. Guest Editorial Special Issue on Security, Privacy, and Trustworthiness in Intelligent Cyber–Physical Systems and Internet of Things[J]. IEEE Internet of Things Journal, 2022, 9(22): 22044-22047.
60. Li Y, Wei X, Li Y, et al. Detection of False Data Injection Attacks in Smart Grid: A Secure Federated Deep Learning Approach[J]. IEEE Transactions on Smart Grid, 2022, 13(6): 4862-4872.
61. Kumar K N, Mohan C K, Cenkeramaddi L R. The impact of adversarial attacks on federated learning: A survey[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2023, 46(5): 2672-2691.
62. Chen J, Zhao Y, Li Q, et al. FedDef: defense against gradient leakage in federated learning-based network intrusion detection systems[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 4561-4576.
63. Li Y, Bu F, Li Y, et al. Optimal scheduling of island integrated energy systems considering multi-uncertainties and hydrothermal simultaneous transmission: A deep reinforcement learning approach[J]. Applied Energy, 2023, 333: 120540.
64. Sun S, Hossain-McKenzie S, Al Homoud L, et al. An AI-based Approach for Scalable Cyber-Physical Optimal Response in Power Systems[C]//2024 IEEE Texas Power and Energy Conference (TPEC). IEEE, 2024: 1-6.
65. Fan X, Du L, Duan D. Synchrophasor Data Correction Under GPS Spoofing Attack: A State Estimation-Based Approach[J]. IEEE Transactions on Smart Grid, 2018, 9(5): 4538-4546.
66. Wan Y, Cao J. A brief survey of recent advances and methodologies for the security control of complex cyber–physical networks[J]. Sensors, 2023, 23(8): 4013.
67. Shenoy D, Bhat R, Krishna Prakasha K. Exploring privacy mechanisms and metrics in federated learning[J]. Artificial Intelligence Review, 2025, 58(8): 223.
68. Li Y, Wei X, et al. Detection of false data injection attacks in smart grid: A secure federated deep learning approach[J]. IEEE Transactions on Smart Grid, 2022, 13(6): 4862–4872.
69. Khaitan S K, McCalley J D. Cyber physical system approach for design of power grids: A survey[C]//2013 IEEE Power & Energy Society General Meeting. IEEE, 2013: 1-5.
70. He S, Li Y, et al. Boosting communication efficiency in federated learning for multiagent-based multimicrogrid energy management[J]. IEEE Transactions on Neural Networks and Learning Systems, 2025, 36(5): 8592–8605.
71. Banik S, Ramachandran T, Bhattacharya A, et al. Automated adversary-in-the-loop cyber-physical defense planning[J]. ACM Transactions on Cyber-Physical Systems, 2023, 7(3): 1-25.
72. Jain H, Kumar M, Joshi A M. Intelligent energy cyber physical systems (iECPS) for reliable smart grid against energy theft and false data injection[J]. Electrical Engineering, 2022, 104(1): 331-346.
73. Li Y, Li J, Wang Y, et al. Privacy-preserving spatiotemporal scenario generation of renewable energies: A federated deep generative learning approach[J]. IEEE Transactions on Industrial Informatics, 2022, 18(4): 2310–2320.

 doi:10.20944/preprints202506.0088.v1

74. Sridhar S, Hahn A, Govindarasu M. Cyber-Physical System Security for the Electric Power Grid[J]. Proceedings of the IEEE, 2012, 100(1): 210-224.
75. Lü Y, Zhang X, Wang R, et al. Application and prospect of federated learning in new power systems[J]. Integrated Intelligent Energy, 2024, 46(11): 21-30.
76. Xiong X, Hu S, Sun D, et al. Detection of false data injection attack in power information physical system based on SVM-GAB algorithm[J]. Energy Reports, 2022, 8(5): 1156-1164.
77. Huang H, Wlazlo P, Mao Z, et al. Cyberattack defense with cyber-physical alert and control logic in industrial controllers[J]. IEEE Transactions on Industry Applications, 2022, 58(5): 5921-5934.
78. Qu Z, Shi H, Wang Y, et al. Active and Passive Defense Strategies of Cyber-Physical Power System against Cyber Attacks Considering Node Vulnerability[J]. Processes, 2022, 10(7): 1351.
79. Presekal A, Ştefanov A, Semertzis I, et al. Spatio-temporal advanced persistent threat detection and correlation for cyber-physical power systems using enhanced GC-LSTM[J]. IEEE Transactions on Smart Grid, 2024.
80. Chen Y, Huang S, Liu F, et al. Evaluation of Reinforcement Learning-Based False Data Injection Attack to Automatic Voltage Control[J]. IEEE Transactions on Smart Grid, 2019, 10(2): 2158-2169.
81. Park K, Hong J, Su W, et al. Machine Learning based Post Event Analysis for Cybersecurity of Cyber-Physical System[C]//2024 IEEE Power & Energy Society General Meeting (PESGM). IEEE, 2024: 1-5.
82. Li Y, Zhang S, Li Y, et al. PMU Measurements-Based Short-Term Voltage Stability Assessment of Power Systems via Deep Transfer Learning[J]. IEEE Transactions on Instrumentation and Measurement, 2023, 72: 2526111.
83. Sun J, et al. Indicator & crowding distance-based evolutionary algorithm for combined heat and power economic emission dispatch[J]. Applied Soft Computing, 2020, 90: 106158.
84. Yang F, Wang J, Pan Q, et al. Resilient Event-Triggered Control for Cyber-Physical Integrated Power Systems Under Network Attacks[J]. Acta Automatica Sinica, 2019, 45(1): 110-119.
85. Chen L, Li Y, Huang M, et al. Robust Dynamic State Estimator of Integrated Energy Systems Based on Natural Gas Partial Differential Equations[J]. IEEE Transactions on Industry Applications, 2022, 58(3): 3303-3312.
86. Susuki Y, Koo T, Ebina H, et al. A Hybrid System Approach to the Analysis and Design of Power Grid Dynamic Performance[J]. Proceedings of the IEEE, 2012, 100(1): 225-239.
87. Song M, Zhou J, Gao C, et al. Coordinated operation of urban buildings and distribution networks from a CPSS perspective: A review and outlook[J]. Automation of Electric Power Systems, 2023, 47(23): 105–121.
88. Liu X, Li Z, Shuai Z, et al. Cyber Attacks Against the Economic Operation of Power Systems: A Fast Solution[J]. IEEE Transactions on Smart Grid, 2017, 8(2): 1023-1025.
89. Wei L, Zhang Q. Detection of False Data Attacks in Smart Grids Based on Improved UKF[J]. Journal of System Simulation, 2023, 35(7): 1508.
90. Guo S, Liu Y, Shao S, et al. Security boundary protection technology for cross-domain data circulation in new power systems[J]. Automation of Electric Power Systems, 2024, 48(6): 96–111.
91. Nasir Z U I, Iqbal A, Qureshi H K. Securing cyber-physical systems: A decentralized framework for collaborative intrusion detection with privacy preservation[J]. IEEE Transactions on Industrial Cyber-Physical Systems, 2024.
92. Li Y, Ma W, Li Y, et al. Enhancing Cyber-Resilience in Integrated Energy System Scheduling with Demand Response Using Deep Reinforcement Learning[J]. Applied Energy, 2025, 379:124831.
93. Wang B, Zhu J, Wang J, et al. A federated learning-based framework for industry load forecasting under smart meter data privacy protection[J]. Automation of Electric Power Systems, 2023, 47(13): 86–93.
94. Xu S, Xia Y, Shen H L. Cyber protection for malware attack resistance in cyber-physical power systems[J]. IEEE Systems Journal, 2022, 16(4): 5337-5345.
95. Alvarez-Alvarado M S, Apolo-Tinoco C, Ramirez-Prado M J, et al. Cyber-physical power systems: A comprehensive review about technologies drivers, standards, and future perspectives[J]. Computers and Electrical Engineering, 2024, 116: 109149.
96. Kong X, Lu Z, Guo X, et al. Resilience evaluation of cyber-physical power system considering cyber attacks[J]. IEEE Transactions on Reliability, 2023, 73(1): 245-256.

 doi:10.20944/preprints202506.0088.v1

97. Chen L, Wang B. Robustness assessment of weakly coupled cyber-physical power systems under multi-stage attacks[J]. Electric Power Systems Research, 2024, 231: 110325.
98. Luo X, He J, Wang X, et al. Topology Optimization for Resilient Defense Strategies Against False Data Injection Attacks in Smart Grids[J]. Acta Automatica Sinica, 2023, 49(6): 1326-1338.
99. Deng R, Zhuang P, Liang H. CCPA: Coordinated Cyber-Physical Attacks and Countermeasures in Smart Grid[J]. IEEE Transactions on Smart Grid, 2017, 8(5): 2420-2430.
100. Ren Q, Xiong X, Liu J, et al. Research on digital twin technology in cyberspace security[J]. Journal of System Simulation, 2024, 36(8): 1944-1952.
101. Risbud P, Gatsis N, Taha A. Vulnerability Analysis of Smart Grids to GPS Spoofing[J]. IEEE Transactions on Smart Grid, 2019, 10(4): 3535-3548.
102. Alabadi M, Albayrak Z. Q-learning for securing cyber-physical systems: a survey[C]//2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). IEEE, 2020: 1-13.
103. Huang D, Wang Y, Hu A, et al. False Data Injection Attack Detection Combining Unsupervised and Supervised Learning[J]. Electric Power Engineering Technology, 2024, 43(2): 134-141.
104. Mortlock T, Al Faruque M A. Adaptive Data Fusion for State Estimation and Control of Power Grids Under Attack[J]. IEEE Transactions on Industrial Informatics, 2024.
105. Sheng Y, Guo Q, Xue Y, et al. Modeling and collaborative optimization of power-transportation coupled networks from a cyber-physical-social perspective[J]. Automation of Electric Power Systems, 2024, 48(7): 62–85.
106. Chen L, Hui X, et al. Dynamic state estimation for integrated natural gas and electric power systems[C]//2021 IEEE/IAS Industrial and Commercial Power System Asia (I&CPS Asia). IEEE, 2021: 397-402.
107. Zhou C, Sun Y, Wang D, et al. A survey on federated learning[J]. Journal of Cybersecurity and Information Security, 2021, 7(5): 77–92.
108. Ali M, Sun W. Securing Critical Infrastructures: Restoration from Cyber-Physical Attacks in Active Distribution Grids[C]//2024 IEEE Power & Energy Society General Meeting (PESGM). IEEE, 2024: 1-5.
109. Fan Q, Liu D, Wang Y, et al. Key Technologies and Progress in the Morphological Evolution of Power Cyber-Physical Systems[J]. Proceedings of the CSEE, 2023, 44(21): 8341-8352.
110. He Z, Gao S, Wei X, et al. Research on Attack-Defense Game Model of False Topology Attacks with Branch and Protection Coordination[J]. Power System Technology, 2022, 46(11): 4346-4355.
111. Li X, Yi L, Liu C, et al. Data-Driven Detection of False Data Injection Attacks in Power Systems[J]. Smart Power, 2023, 51(2): 30-37.
112. Weng P, Chen B, Yu L. Fusion Estimation of False Data Injection Attack Signals[J]. Acta Automatica Sinica, 2021, 47(9): 2292-2300.
113. Patel C D, Aggarwal M, Chaubey N K. Enhancing Cyber-Physical Systems Security Through Advanced Defense Mechanisms[M]//Advancing Cyber Security Through Quantum Cryptography. IGI Global, 2025: 307-342.
114. Krishnaveni S, Chen T M, Sathiyanarayanan M, et al. CyberDefender: an integrated intelligent defense framework for digital-twin-based industrial cyber-physical systems[J]. Cluster Computing, 2024, 27(6): 7273-7306.
115. Purohit S, Neupane R, Bhamidipati N R, et al. Cyber threat intelligence sharing for co-operative defense in multi-domain entities[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 20(5): 4273-4290.
116. Zhou X, Feng J, et al. Non-intrusive load decomposition based on CNN–LSTM hybrid deep learning model[J]. Energy Reports, 2021, 7: 5762-5771.
117. Yan B, Yao P, Wang J, et al. Game theoretical dynamic cybersecurity defense strategy for electrical cyber physical systems[C]//2021 IEEE 5th Conference on Energy Internet and Energy System Integration (EI2). IEEE, 2021: 2392-2397.
118. Zhou Z, Zhang J, Zhang X. A review on defense mechanism against the denial of service and false data injection in cyber-physical power systems[C]//2023 IEEE 6th International Electrical and Energy Conference (CIEEC). IEEE, 2023: 4539-4545.

 doi:10.20944/preprints202506.0088.v1

119. Fahmeeda S, Bhagyashree B K. Detection and prevention of false data injection attack in cyber physical power system[C]//2021 IEEE International Conference on Mobile Networks and Wireless Communications (ICMNWC). IEEE, 2021: 1-5.
120. Yang J. A controllable false data injection attack for a cyber physical system[J]. IEEE Access, 2021, 9: 6721-6728.
121. Xing W, Shen J. Security Control of Cyber–Physical Systems under Cyber Attacks: A Survey[J]. Sensors, 2024, 24(12): 3815.
122. Yang J. A controllable false data injection attack for a cyber physical system[J]. IEEE Access, 2021, 9: 6721-6728.
123. Luo D, Xu R, Guan Z. Differential privacy budget optimization method based on deep learning in the Internet of Things environment[J]. Journal of Internet of Things, 2022, 6(2): 65–76.
124. Wang S, Ko R K L, Bai G, et al. Evasion attack and defense on machine learning models in cyber-physical systems: A survey[J]. IEEE communications surveys & tutorials, 2023, 26(2): 930-966.
125. Li Y, Li Z, Chen L. Dynamic State Estimation of Generators Under Cyber Attacks[J]. IEEE Access, 2019, 7: 125252-125267.
126. Xiao K, Zhu C, Xie J, et al. Dynamic defense against stealth malware propagation in cyber-physical systems: a game-theoretical framework[J]. Entropy, 2020, 22(8): 894.
127. Zhao Z, Shang Y, Qi B, et al. Research on defense strategies for power system frequency stability under false data injection attacks[J]. Applied Energy, 2024, 371: 123711.
128. Xiong X, Hu S, Sun D, et al. Detection of false data injection attack in power information physical system based on SVM–GAB algorithm[J]. Energy Reports, 2022, 8: 1156-1164.
129. Qu Z, Xie Q, Liu Y, et al. Power Cyber-Physical System Risk Area Prediction Using Dependent Markov Chain and Improved Grey Wolf Optimization[J]. IEEE Access, 2020, 8: 82844-82854.
130. Zhong C, Li H, Zhou Y, et al. Virtual synchronous generator of PV generation without energy storage for frequency support in autonomous microgrid[J]. International Journal of Electrical Power & Energy Systems, 2022, 134: 107343.
131. Li Y, Zhang M, Chen C. A deep-learning intelligent system incorporating data augmentation for short-term voltage stability assessment of power systems[J]. Applied Energy, 2022, 308: 118347.
132. Costilla-Enriquez N, Weng Y. Attack power system state estimation by implicitly learning the underlying models[J]. IEEE Transactions on Smart Grid, 2022, 14(1): 649-662.
133. Chu X, Yi Y, Tang M, et al. Defensive resource allocation for cyber-physical systems in global energy interconnection[C]//IOP Conference Series: Earth and Environmental Science. IOP Publishing, 2019, 227(4): 042002.
134. Khalid H, Peng J. Immunity Toward Data-Injection Attacks Using Multisensor Track Fusion-Based Model Prediction[J]. IEEE Transactions on Smart Grid, 2017, 8(2): 697-707.
135. Liu X, Chang P, Sun Q. Detection of False Data Injection Attacks in Power Grids Based on XGBoost and Unscented Kalman Filter Adaptive Hybrid Prediction[J]. Proceedings of the CSEE, 2021, 41(16): 5462-5476.
136. Alsharif G O, Anagnostopoulos C, Marnerides A K. Energy Market Manipulation via False-Data Injection Attacks[J]. IEEE Access, 2025.
137. Zhou B, Sun B, Zang T, et al. Security risk assessment approach for distribution network cyber physical systems considering cyber attack vulnerabilities[J]. Entropy, 2022, 25(1): 47.
138. Le J, Lang H, Tan T, et al. A Review of Information Security Issues in Distributed Economic Dispatch of New Distribution Systems[J]. Automation of Electric Power Systems, 2024, 48(12): 177-191.
139. Jiang Z, Yao P, Yan B, et al. Cyber-physical system defense decision-making based on priori knowledge of traffic anomaly detection[C]//2023 IEEE 7th Conference on Energy Internet and Energy System Integration (EI2). IEEE, 2023: 5196-5201.
140. Zideh M J, Khalghani M R, Solanki S K. An unsupervised adversarial autoencoder for cyber attack detection in power distribution grids[J]. Electric Power Systems Research, 2024, 232: 110407.
141. Zhang Z, Huang S, Chen Y, et al. Cyber-physical coordinated risk mitigation in smart grids based on attack-defense game[J]. IEEE Transactions on Power Systems, 2021, 37(1): 530-542.

 doi:10.20944/preprints202506.0088.v1

142. Shafae M S, Wells L J, Purdy G T. Defending against product-oriented cyber-physical attacks on machining systems[J]. The International Journal of Advanced Manufacturing Technology, 2019, 105: 3829-3850.
143. Long X, Ding Y, et al. Privacy-Preserving Graph Inference Network for Multi-Entity Wind Power Forecast: A Federated Learning Approach[J]. IEEE Transactions on Network Science and Engineering, 2025. DOI: 10.1109/TNSE.2025.3547227.
144. Lian Z, Shi P, Chen M. A Survey on Cyber-Attacks for Cyber-Physical Systems: Modeling, Defense and Design[J]. IEEE Internet of Things Journal, 2024.
145. Qu Z, Dong Y, Li Y, et al. Localization of Dummy Data Injection Attacks in Power Systems Considering Incomplete Topological Information: A Spatio-Temporal Graph Wavelet Convolutional Neural Network Approach[J]. Applied Energy, 2024, 360: 122736.
146. Liu S, Tan Y, Zhao F, et al. Coupled Modeling Method for Power Information Systems[J]. Journal of Power Systems and Automation, 2021, 33(3): 89-93.
147. Yang T, Cai S, Yan P, et al. Saturation defense method of a power cyber-physical system based on active cut set[J]. IEEE Transactions on Smart Grid, 2022.
148. Liu X, Bao Z, Lu D, et al. Modeling of Local False Data Injection Attacks With Reduced Network Information[J]. IEEE Transactions on Smart Grid, 2015, 6(4): 1686-1696.
149. Li Y, Wang R, Li Y, et al. Wind power forecasting considering data privacy protection: A federated deep reinforcement learning approach[J]. Applied Energy, 2023, 329: 120291.
150. Khanna K, Govindarasu M. Resiliency-driven cyber–physical risk assessment and investment planning for power substations[J]. IEEE Transactions on Control Systems Technology, 2024, 32(5): 1743-1754.
151. Sun S, Huang H, Payne E, et al. A graph embedding-based approach for automatic cyber-physical power system risk assessment to prevent and mitigate threats at scale[J]. IET Cyber-Physical Systems: Theory & Applications, 2024, 9(4): 435-453.
152. Jin Z, Liu Y, Diao J, et al. Covert False Data Injection Attacks on Remote State Estimation in Cyber-Physical Systems[J]. Acta Automatica Sinica, 2025, 51(2): 1-10.
153. Shi J, Chen B, Yu L. Hidden FDIA Detection Based on Laplacian Eigenmap Learning[J]. Acta Automatica Sinica, 2021, 47(10): 2494-2500.
154. Ribas Monteiro L F, Rodrigues Y R, Zambroni de Souza A C. Cybersecurity in cyber–physical power systems[J]. Energies, 2023, 16(12): 4556.
155. Qu Z, Bo X, Yu T, et al. Active and Passive Hybrid Detection Method for Power CPS False Data Injection Attacks with Improved AKF and GRU-CNN[J]. IET Renewable Power Generation, 2022, 16: 1490-1508. DOI: 10.1049/rpg2.12432.
156. Shen Y, Zhang W, Ni H, et al. Guaranteed Cost Control of Networked Control Systems with DoS Attack and Time-varying Delay[J]. International Journal of Control, Automation and Systems, 2019, 17(4): 811-821.
157. Liu S, Martínez S, Cortés J. Stabilization of linear cyber-physical systems against attacks via switching defense[J]. IEEE Transactions on Automatic Control, 2023, 68(12): 7326-7341.
158. Liang Y, Wang Y, Liu K, et al. Fault Simulation of Distribution Grid CPS Considering Network Information Security[J]. Power System Technology, 2020, 45(1): 235-242.
159. Barrère M, Hankin C, O'Reilly D. Cyber-physical attack graphs (CPAGs): Composable and scalable attack graphs for cyber-physical systems[J]. Computers & security, 2023, 132: 103348.
160. Manias D M, Saber A M, Radaideh M I, et al. Trends in Smart Grid Cyber-Physical Security: Components, Threats and Solutions[J]. IEEE Access, 2024. Fu Y, Chen L, Ma Z, et al. Preventive Control of Power Systems Including Data-Driven Stability Constraints[J]. Proceedings of the CSEE, 2022, 42(15): 5417-5430.
161. Feng Y, Huang R, Zhao W, et al. A survey on coordinated attacks against cyber–physical power systems: Attack, detection, and defense methods[J]. Electric Power Systems Research, 2025, 241: 111286.
162. Li B, Xiao Y, Shi Y, et al. Anti-honeypot enabled optimal attack strategy for industrial cyber-physical systems[J]. IEEE Open Journal of the Computer Society, 2020, 1: 250-261.
163. Li T, Zhao H, Wang S, et al. Attack and Defense Strategy of Distribution Network Cyber-Physical System Considering EV Source-Charge Bidirectionality[J]. Electronics, 2021, 10(23): 2973.
164. Lei C, Bu S, Wang Q, et al. Observability defense-constrained distribution network reconfiguration for cyber-physical security enhancement[J]. IEEE Transactions on Smart Grid, 2023, 15(2): 2379-2382.

 doi:10.20944/preprints202506.0088.v1

165. Zhu W, Tang Y, Wei X, et al. Defense methods against adversarial attacks on data-driven algorithms in power CPS[J]. Electric Power, 2024, 57(9): 285-294.
166. Cui Y, et al. Deep reinforcement learning based optimal energy management of multi-energy microgrids with uncertainties[J]. CSEE Journal of Power and Energy Systems, 2024: 1-12. DOI: 10.17775/CSEEJPES.2023.05120.
167. Ao W, Song Y, Wen C. Adaptive cyber-physical system attack detection and reconstruction with application to power systems[J]. IET Control Theory & Applications, 2016, 10(12): 1458-1468.
168. Yang X, et al. Gaussian Mixture Model Uncertainty Modeling for Power Systems Considering Mutual Assistance of Latent Variables[J]. IEEE Transactions on Sustainable Energy, 2024, 1-4. DOI: 10.1109/TSTE.2024.3356259.
169. Barrère M, Hankin C, O'Reilly D. Cyber-physical attack graphs (CPAGs): Composable and scalable attack graphs for cyber-physical systems[J]. Computers & security, 2023, 132: 103348.
170. Setitra M, Fan M, Benkhaddra I. DoS/DDoS Attacks in Software Defined Networks: Current Situation, Challenges and Future Directions[J]. Computers and Communications, 2024, 222: 77-96.
171. Wei J, Yan X, Zhu X, Xu M, Ma R, Du H. New Stability Conditions of CPSs with Multiple Transportation Channels under DoS Attacks[J]. Science China Information Sciences, 2022, 65(11): 219202.
172. Xiao Y, Chai S, Dai L, Xia Y, Chai R. Stochastic Tube-Based Model Predictive Control for Cyber-Physical Systems under False Data Injection Attacks with Bounded Probability[J]. arXiv preprint arXiv:2503.07385, 2025.
173. Alguliyev R, Imamverdiyev Y, Sukhostat L. Cyber-Physical Systems and Their Security Issues[J]. Computers in Industry, 2018, 100: 212-223.
174. Jeong S, Baek Y, Son S. Component-Based Interactive Framework for Intelligent Transportation Cyber-Physical Systems[J]. Sensors, 2020, 20(1): 264.
175. Song S, Park J H, Zhang B, Song X. Event-Based Adaptive Fuzzy Fixed-Time Secure Control for Nonlinear CPSs Against Unknown False Data Injection and Backlash-Like Hysteresis[J]. IEEE Transactions on Fuzzy Systems, 2022, 30(6): 1939-1951.
176. Li Y, Wei X, Li Y, Dong Z, Shahidehpour M. Detection of False Data Injection Attacks in Smart Grid: A Secure Federated Deep Learning Approach[J]. arXiv preprint arXiv:2209.00778, 2022.
177. Zhao H J, Li Q Z, Zeng X, Liu Z M. Safe Reinforcement Learning Algorithm and Its Application in Intelligent Control for CPS[J]. International Journal of Software and Informatics, 2022, 12(4): 453-483.
178. Hasan M, Habib A, Shukur Z, Ibrahim F, Islam S, Razzaque M A. Review on Cyber-Physical and Cyber-Security System in Smart Grid: Standards, Protocols, Constraints, and Recommendations[J]. Journal of Network and Computer Applications, 2023, 209: 103540.
179. Li Y, Yang Z. Application of EOS-ELM with Binary Jaya-Based Feature Selection to Real-Time Transient Stability Assessment Using PMU Data[J]. IEEE Access, 2017, 5: 23092-23101.
180. Ye D, Zhang T. Summation Detector for False Data-Injection Attack in Cyber-Physical Systems[J]. IEEE Transactions on Cybernetics, 2019, 50(6): 2338-2345.
181. Eslami A, Khorasani K. Zero Dynamics Attack Detection and Isolation in Cyber-Physical Systems with Event-Triggered Communication[J]. arXiv preprint arXiv:2505.06070, 2025.
182. Razaque A, Amsaad F H, Abdulgader M, Alotaibi B, Alsolami F, Gulsezim D. A Mobility-Aware Human-Centric Cyber-Physical System for Efficient and Secure Smart Healthcare[J]. IEEE Internet of Things Journal, 2022, 9(22): 22434-22452.
183. Xue K. Securing Power Cyber-Physical Systems Against False Data Injection Attacks: Trends, Techniques, and Future Directions[J]. Preprints, 2025.
184. Chattopadhyay A, Mitra U. Security Against False Data-Injection Attack in Cyber-Physical Systems[J]. IEEE Transactions on Control of Network Systems, 2019, 7(2): 1015-1027.
185. Koley I, Adhikary S, Dey S. An RL-Based Adaptive Detection Strategy to Secure Cyber-Physical Systems[J]. arXiv preprint arXiv:2103.02872, 2021.
186. Zhang X, Han H. Event-Triggered Finite-Time Filtering for Nonlinear Networked System with Quantization and DoS Attacks[J]. IEEE Access, 2024, 12: 1308-1320.

 doi:10.20944/preprints202506.0088.v1

187. Rieger C G, Gertman D I, McQueen M A. Resilient Control Systems: Next Generation Design Research[J]. 2nd IEEE Conference on Human System Interaction, 2009: 632-636.
188. Rinaldi S M, Peerenboom J P, Kelly T K. Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies[J]. IEEE Control Systems Magazine, 2001, 21(6): 11-25.
189. Rinaldi S M, Peerenboom J P, Kelly T K. Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies[J]. IEEE Control Systems Magazine, 2001, 21(6): 11-25.
190. Sun C, Su Q, Li J. Secure Tracking Control and Attack Detection for Power Cyber-Physical Systems based on Integrated Control Decision[J]. IEEE Transactions on Information Forensics and Security, 2024.
191. Wang P, Zhang R, He X. New Approaches to Detection and Secure Control for Cyber-physical Systems Against False Data Injection Attacks[J]. International Journal of Control, Automation and Systems, 2025, 23(1): 332-345.
192. Kaloudi N, Li J. The ML-based sensor data deception targeting cyber–physical systems: A review[J]. Computer Science Review, 2025, 57: 100753.
193. Busari W A, Bello A A. Security, Trust, and Privacy in Cyber-physical Systems (CPS)[C]//2024 2nd International Conference on Cyber Physical Systems, Power Electronics and Electric Vehicles (ICPEEV). IEEE, 2024: 1-6.
194. Noor U, Shahid S, Kanwal R, et al. A Machine Learning based Empirical Evaluation of Cyber Threat Actors High Level Attack Patterns over Low level Attack Patterns in Attributing Attacks[J]. arXiv preprint arXiv:2307.10252, 2023.
195. Samad T. Human-in-the-loop control and cyber–physical–human systems: applications and categorization[J]. Cyber–physical–human systems: fundamentals and applications, 2023: 1-23.
196. Gil M, Albert M, Fons J, et al. Engineering human-in-the-loop interactions in cyber-physical systems[J]. Information and software technology, 2020, 126: 106349.
197. Iyenghar P. Clever Hans in the Loop? A Critical Examination of ChatGPT in a Human-in-the-Loop Framework for Machinery Functional Safety Risk Analysis[J]. Eng, 2025, 6(2): 31.
198. Adil M, Farouk A, Abulkasim H, et al. NG-ICPS: Next Generation Industrial-CPS, Security Threats in the Era of Artificial Intelligence, Open Challenges With Future Research Directions[J]. IEEE Internet of Things Journal, 2024.
199. Agarwal M, Venkateswaran S K, Sivakumar R. Human-in-the-loop rl with an eeg wearable headset: On effective use of brainwaves to accelerate learning[C]//Proceedings of the 6th ACM Workshop on Wearable Systems and Applications. 2020: 25-30.
200. Nguyen T T, Kadavil R, Hooshyar H. A Real-time Cyber-Physical Simulation Testbed for Cybersecurity Assessment of Large-Scale Power Systems[J]. IEEE Transactions on Industry Applications, 2024.
201. Li P, Fu J, Xie K, et al. A Defense Planning Model for a Power System Against Coordinated Cyber-Physical Attack[J]. Protection and Control of Modern Power Systems, 2024, 9(5): 84-95.
202. Ravikumar G, Hyder B, Babu J R, et al. Cps testbed architectures for wampac using industrial substation and control center platforms and attack-defense evaluation[C]//2021 IEEE Power & Energy Society General Meeting (PESGM). IEEE, 2021: 1-5.
203. Jiang Y, Wu S, Ma R, et al. Monitoring and defense of industrial cyber-physical systems under typical attacks: From a systems and control perspective[J]. IEEE Transactions on Industrial Cyber-Physical Systems, 2023, 1: 192-207.
204. Fan Y, Li J, Zhang D, et al. Supporting sustainable maintenance of substations under cyber-threats: An evaluation method of cybersecurity risk for power CPS[J]. Sustainability, 2019, 11(4): 982.
205. Chen Y, Li T, Long Y, Bai W. Attacks Detection and Security Control for Cyber-Physical Systems under False Data Injection Attacks[J]. Journal of The Franklin Institute, 2023, 360(14): 10476-10498.
206. Abdelmalak M. Effects of Unobservable Bus States on Detection and Localization of False Data Injection Attacks in Smart Grids[D]. University of South Florida, 2024.
207. Feng H, Han Y, Si F, Zhao Q. Detection of False Data Injection Attacks in Cyber-Physical Power Systems: An Adaptive Adversarial Dual Autoencoder with Graph Representation Learning Approach[J]. IEEE Transactions on Instrumentation and Measurement, 2024, 73: 1-11.

 doi:10.20944/preprints202506.0088.v1

208. Guan Y, Ge X. Distributed Attack Detection and Secure Estimation of Networked Cyber-Physical Systems Against False Data Injection Attacks and Jamming Attacks[J]. IEEE Transactions on Signal and Information Processing over Networks, 2017, 4(1): 48-59.
209. Barboni A, Rezaee H, Boem F, Parisini T. Detection of Covert Cyber-Attacks in Interconnected Systems: A Distributed Model-Based Approach[J]. IEEE Transactions on Automatic Control, 2020, 65(9): 3728-3741.
210. Li Y, Li J, Wang Y. Privacy-preserving spatiotemporal scenario generation of renewable energies: A federated deep generative learning approach[J]. IEEE Transactions on Industrial Informatics, 2021, 18(4): 2310-2320.
211. [212 Majidi S H, Asharioun H. Privacy preserving federated learning solution for security of industrial cyber physical systems[J]. AI-Enabled Threat Detection and Security Analysis for Industrial IoT, 2021: 195-211.
212. Yan K, Liu X, Lu Y, et al. A cyber-physical power system risk assessment model against cyberattacks[J]. IEEE Systems Journal, 2022, 17(2): 2018-2028.
213. Kausar F, Deo S, Hussain S, et al. Federated Deep Learning Model for False Data Injection Attack Detection in Cyber Physical Power Systems[J]. Energies, 2024, 17(21): 5337.
214. Fang Z, Zhao D, Chen C, et al. Nonintrusive Appliance Identification with Appliance-Specific Networks[J]. IEEE Transactions on Industry Applications, 2020, 56(4): 3443-3452.
215. BaSin D, Cremers C, Kim T, et al. Design, Analysis, and Implementation of ARPKI: an Attack-Resilient Public-Key Infrastructure[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 15(3): 393-408.
216. Li Y, Li J, Qi J, et al. Robust Cubature Kalman Filter for Dynamic State Estimation of Synchronous Machines Under Unknown Measurement Noise Statistics[J]. IEEE Access, 2019, 7: 29139-29148.
217. Bai M, Liu P, Lv F, et al. Adversarial Attack against Intrusion Detectors in Cyber-Physical Systems With Minimal Perturbations[C]//2024 IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA). IEEE, 2024: 816-825.
218. Preeti G, Sanjeev Kumar P. A Blockchain Based Decentralized Application System for Vanet FDIA Detection[C]//International Conference on Computing and Communication Networks. Singapore: Springer Nature Singapore, 2023: 95-119.
219. Xu K, Niu Y. Decentralized attack detection for multi-area power systems via interconnection-decoupled sliding mode observer[J]. International Journal of Robust and Nonlinear Control, 2023, 33(12): 6697-6714.
220. Dong Z, Tang M, Tian M. Allocating defense resources for spatial cyber-physical power systems based on deep reinforcement learning[C]//2023 IEEE 6th International Conference on Industrial Cyber-Physical Systems (ICPS). IEEE, 2023: 1-6.
221. Cui P, Cui M, Wang Q, et al. Identification method of coordinated cyber-PV ramping attacks based on tensor decomposition personalized federated learning[J]. Transactions of China Electrotechnical Society, 2025, 50(1): 15-24.
222. Ullrich J, Weippl E R. CyPhySec: Defending cyber-physical systems[J]. ERCIM News, 2015, 102: 18-18.
223. Zhang F, Huang Z, Kou L, et al. Data Encryption Based on a 9D Complex Chaotic System with Quaternion for Smart Grid[J]. Chinese Physics B, 2023, 32(1): 010502.
224. Zhong X, xin Li G, Zhng C. False data injection in power smart grid and identification of the most vulnerable bus; a case study 14 IEEE bus network[J]. Energy Reports, 2021, 7: 8476-8484.
225. Qu Z, Dong Y, Mugemanyi S, et al. Dynamic Exploitation Gaussian Bare-Bones Bat Algorithm for Optimal Reactive Power Dispatch to Improve the Safety and Stability of Power System[J]. IET Renewable Power Generation, 2022, 16: 1401-1424.
226. Keçeci C, Davis K R, Serpedin E. Federated learning based distributed localization of false data injection attacks on smart grids[J]. arXiv preprint arXiv:2306.10420, 2023.
227. War M R, Singh Y, Sheikh Z A, et al. Review on the Use of Federated Learning Models for the Security of Cyber-Physical Systems[J]. Scalable Computing: Practice and Experience, 2025, 26(1): 16-33.
228. Shafi S, Tariq N, Khan F A, et al. Federated Learning for Enhanced Malware Threat Detection to Secure Smart Power Grids[C]//International Conference on Ubiquitous Computing and Ambient Intelligence. Cham: Springer Nature Switzerland, 2024: 692-703.

 doi:10.20944/preprints202506.0088.v1

229. Singh N K, Patni S, Lim S, et al. Federated Learning-Based Secure Computing Mechanism for Consumer Internet of Vehicles-based Transportation Cyber-Physical Systems[J]. IEEE Transactions on Consumer Electronics, 2025.
230. Khraisat A, Alazab A, Singh S, et al. Survey on federated learning for intrusion detection system: Concept, architectures, aggregation strategies, challenges, and future directions[J]. ACM Computing Surveys, 2024, 57(1): 1-38.
231. Yogi M K, Chakravarthy A S N. Privacy-Preserving Deep Reinforcement Learning for Secure Resource Orchestration in Cyber-Physical Systems[J]. International Journal of Scientific Research in Network Security and Communication, 2025, 13(2): 12-21.
232. Raza M, Saeed M J, Riaz M B, et al. Federated learning for privacy preserving intrusion detection in software defined networks[J]. IEEE Access, 2024.
233. Lei S, Xia X, Sha J. Day-ahead Demand Response Potential Forecasting Method for Data Centers Based on Federated Learning[C]//2024 IEEE/IAS Industrial and Commercial Power System Asia (I&CPS Asia). IEEE, 2024: 490-495.
234. Soomro I A, Hussain S J, Ashraf Z, et al. Lightweight privacy-preserving federated deep intrusion detection for industrial cyber-physical system[J]. Journal of Communications and Networks, 2024, 26(6): 632-649.
235. Mahmud S A, Islam N, Islam Z, et al. Privacy-Preserving Federated Learning-Based Intrusion Detection Technique for Cyber-Physical Systems[J]. Mathematics, 2024, 12(20): 3194.
236. Su Y, Fan W, Meng Q, et al. Joint Adaptive Aggregation and Resource Allocation for Hierarchical Federated Learning Systems Based on Edge-Cloud Collaboration[J]. IEEE Transactions on Cloud Computing, 2025, 13(1): 369 - 382.
237. Popli M S, Singh R P, Popli N K, et al. A Federated Learning Framework for Enhanced Data Security and Cyber Intrusion Detection in Distributed Network of Underwater Drones[J]. IEEE Access, 2025, 13: 12634-12646.