Machine Learning Techniques for Enhancing Cyber-Physical Systems: A Comprehensive Review

Kushal Patel[1], Pooja Patel[2]

[1] Computer Engineering Department, C. K. Pithawala College of Engineering, Surat, India

[2] Information Technology Department, R. N. G. Patel Institute of Technology, Bardoli, India

DOI : https://doi.org/10.51583/IJLTEMAS.2025.1412000048

Received: 16 December 2025; Accepted: 23 December 2025; Published: 02 January 2026

ABSTRACT

Cyber-Physical Systems (CPS) represent a foundational paradigm shift in modern engineered systems by integrating computation, control, communication, and physical processes into a unified architecture. As CPS rapidly expand across critical domains such as smart grids, industrial automation, and smart agriculture, the growing complexity, dynamicity, and scale of these environments necessitate the adoption of advanced Machine Learning (ML) techniques capable of enabling autonomous decision-making, predictive intelligence, and resilience under uncertainty. This review presents a comprehensive synthesis of ML methodologies applied to CPS, covering supervised, unsupervised, reinforcement, and deep learning paradigms. The paper further examines their domain-specific applications, architectural integration challenges, security implications, deployment issues across edge–fog–cloud infrastructures, and emerging research opportunities. The analysis highlights the indispensable role of ML in shaping next-generation CPS with improved efficiency, robustness, and adaptability.

Keywords— Cyber-Physical Systems (CPS), Machine Learning, Smart Grids, Industrial IoT, Industry 4.0, Smart Agriculture, Deep Learning, Reinforcement Learning, Edge Computing

INTRODUCTION

Cyber-Physical Systems (CPS) have emerged as a fundamental technological paradigm for modern infrastructures by integrating sensing, actuation, networking, and computational intelligence to enable real-time interaction with the physical environment [1], [2]. Unlike traditional embedded systems, CPS exhibit large-scale interconnectedness, strict temporal constraints, and continuous feedback loops between cyber and physical components. These characteristics allow CPS to support a wide range of mission-critical applications, including power distribution, manufacturing automation, healthcare monitoring, transportation systems, and agricultural management [1], [2].

The inherent complexity and heterogeneity of CPS result in massive volumes of multimodal data that conventional rule-based approaches struggle to process effectively. Consequently, Machine Learning (ML) has become indispensable for enhancing CPS intelligence by enabling predictive maintenance, anomaly detection, system optimization, environmental forecasting, cyber-attack mitigation, and autonomous decision-making [3], [5], [6]. The rapid digital transformation driven by Industry 4.0 practices, dense IoT deployments, and advances in high-performance networking and computing infrastructures has further increased reliance on data-driven intelligence within CPS environments [3], [6].

Despite these advantages, integrating ML into CPS introduces significant challenges. Stringent latency requirements, safety and reliability constraints, limited availability of labeled data, lack of model explainability, vulnerability to adversarial attacks, and resource limitations across distributed system layers hinder large-scale deployment of ML-enabled CPS. Addressing these challenges is essential to ensure robust, transparent, and trustworthy system operation [4], [5].

In response, this review presents a comprehensive analysis of ML-driven CPS, covering foundational architectures, core ML techniques, and domain-specific applications in Smart Grids, Industrial IoT, and Smart Agriculture. It further examines ML-based security mechanisms, deployment strategies across edge–fog–cloud environments, and key research challenges, outlining future directions for developing intelligent, resilient, and scalable CPS infrastructures.

CPS Architecture and Fundamental Components

Cyber-Physical Systems (CPS) are characterized by the seamless integration of computation, communication, control, and physical processes to enable intelligent interaction with real-world environments. Their architecture is commonly represented as a multilayered structure in which each layer performs distinct yet interdependent functions. Understanding these architectural components is essential for appreciating how Machine Learning (ML) can be effectively embedded within CPS to enhance intelligence, resilience, and autonomy [1], [2], [5].

At the foundation of CPS lies the physical sensing and actuation layer, which interfaces directly with the environment. Sensors continuously monitor variables such as temperature, voltage, vibration, motion, moisture, and chemical composition, generating real-time data streams for analysis. Actuators execute mechanical or electrical actions based on computed decisions. The quality of sensor data—defined by fidelity, resolution, and sampling frequency—directly affects the reliability of downstream ML tasks, as noisy or inaccurate measurements can significantly degrade model performance [1], [5].

Above the physical layer, the communication and networking layer enables bidirectional information exchange among CPS components. This layer employs heterogeneous communication technologies, including wireless sensor networks, 5G/6G cellular systems, LoRaWAN, ZigBee, MQTT, and industrial Ethernet. High throughput, low latency, and fault tolerance are critical to supporting real-time ML inference and closed-loop control. The distributed nature of CPS also creates opportunities for ML-based network optimization, traffic prediction, congestion control, and communication security [3], [26].

The computational and data processing layer forms the cyber core of CPS, responsible for data aggregation, filtering, transformation, and storage. Depending on application requirements, computation may be centralized in the cloud, decentralized at the edge, or distributed across fog architectures. While ML model training is often performed in cloud environments with abundant computational resources, inference is increasingly executed at the edge to minimize latency and communication overhead. This layer hosts real-time analytics, predictive modeling, and autonomous decision-making pipelines that enable adaptive CPS behavior [26], [27], [28].

The control and decision-making layer integrates ML-driven insights with traditional control-theoretic approaches to ensure system stability, safety, and efficiency. Techniques such as reinforcement learning, model predictive control, and optimization algorithms support dynamic decision processes under uncertainty. In safety-critical domains—including smart grids, industrial automation, and transportation systems—this layer must satisfy strict reliability and regulatory requirements [2], [35].

At the highest level, the application and services layer delivers domain-specific functionalities for Smart Grids, Industrial IoT, Smart Agriculture, healthcare CPS, autonomous vehicles, and smart cities. This layer provides user interfaces, visualization tools, business logic, and enterprise integration, enabling context-aware and secure system operation [6], [7], [15].

Across all layers, CPS require cross-cutting properties such as scalability, interoperability, robustness, and security. While ML enhances fault detection, anomaly analysis, and optimization, it also introduces vulnerabilities related to adversarial attacks, data poisoning, and model interpretability. Consequently, CPS architectures must incorporate mechanisms for data quality assurance, secure communication, model lifecycle management, and distributed intelligence to support reliable ML integration at scale [4], [42], [50]

Machine Learning Techniques for Cyber-Physical Systems

Machine Learning (ML) has emerged as a foundational technology for enhancing the intelligence, adaptability, and operational resilience of Cyber-Physical Systems (CPS). The dynamic, data-intensive, and heterogeneous nature of CPS environments demands analytical models capable of learning complex patterns, predicting system behavior, and responding autonomously to changing operational and environmental conditions. Consequently, ML has become a critical enabler of intelligent CPS operation. This section presents a structured analysis of key ML paradigms—including supervised, unsupervised, reinforcement, and deep learning—while highlighting their applicability to CPS domains. It also discusses ensemble and hybrid learning strategies, model selection considerations, and challenges associated with real-time CPS deployment [31], [32], [35].

A. Supervised Learning for CPS

Supervised learning is widely adopted in CPS due to its effectiveness in modeling input–output relationships using labeled datasets. In Smart Grids, supervised techniques such as Support Vector Machines, Random Forests, and Gradient Boosting Machines are commonly applied for short-term load forecasting, fault diagnosis, power theft detection, and renewable energy generation prediction. In Industrial IoT environments, supervised models support predictive maintenance by analyzing sensor degradation patterns to anticipate machine failures. Similarly, in Smart Agriculture, classifiers such as k-Nearest Neighbors and Decision Trees are used for pest identification, crop disease detection, and yield prediction [13], [18], [21].

Despite its effectiveness, supervised learning faces notable challenges in CPS applications, including limited availability of labeled data, concept drift due to evolving environmental conditions, and noise inherent in sensor measurements. To mitigate these issues, adaptive techniques such as incremental learning, transfer learning, and domain adaptation are increasingly incorporated to enhance robustness and generalization [47], [48].

B. Unsupervised Learning for CPS

Unsupervised learning plays a vital role in CPS scenarios where labeled data is scarce or unavailable. Clustering algorithms such as k-Means, DBSCAN, and hierarchical clustering are widely used for anomaly detection in industrial systems, consumption pattern analysis in energy networks, and behavioral modeling in distributed sensor environments. Dimensionality reduction techniques, including Principal Component Analysis and autoencoders, enable efficient feature extraction from large-scale sensor data, supporting compact representation and reduced computational overhead in resource-constrained CPS [16], [40].

In Smart Agriculture, unsupervised learning supports soil condition segmentation, environmental clustering, and pattern discovery in remote sensing imagery. However, these models often suffer from limited interpretability and sensitivity to noise, making their performance highly dependent on preprocessing quality and parameter selection [22], [24].

C. Reinforcement and Deep Learning for CPS

Reinforcement Learning (RL) enables CPS to learn optimal control strategies through continuous interaction with the environment. RL algorithms such as Q-learning, Deep Q-Networks, and Actor–Critic methods have been applied to voltage regulation in Smart Grids, robotic control in industrial automation, and irrigation management in smart farming systems [11], [35]. Although RL is well suited for long-term optimization under uncertainty, challenges related to safety, sample efficiency, and convergence persist, motivating ongoing research into safe, model-based, and multi-agent RL approaches [35], [50].

Deep Learning (DL) models—including CNNs, RNNs, LSTMs, and Transformers—are extensively used to process high-dimensional CPS data such as time-series signals, images, and multimodal sensor streams [31], [32], [34]. DL has demonstrated strong performance across CPS domains, including load forecasting, defect detection, and crop monitoring [13], [18], [22]. However, high computational requirements limit DL deployment at the edge, prompting the use of model compression, pruning, and TinyML techniques for lightweight inference [30], [26].

Machine Learning Applications in Cyber-Physical Systems

Machine Learning (ML) has emerged as a foundational enabler of intelligence, adaptability, and autonomy in modern Cyber-Physical Systems (CPS) [1]. The continuous, heterogeneous, and dynamic data streams generated by CPS environments require advanced ML techniques to extract patterns, predict system states, detect anomalies, and support optimal decision-making [31]. Since CPS applications differ significantly across domains, ML deployment strategies must be tailored to domain-specific operational constraints, sensing modalities, and performance requirements. This section summarizes ML applications in three major CPS domains: Smart Grids, Industrial IoT (Industry 4.0), and Smart Agriculture.

A. ML Applications in Smart Grids

Smart Grids represent one of the most mature CPS domains, integrating distributed energy resources, sensors, smart meters, and control devices [7], [8]. ML plays a crucial role in enabling real-time monitoring, forecasting, and control within these complex infrastructures.

Load forecasting and demand prediction are among the most critical ML applications in Smart Grids. Models such as LSTM networks, support vector regression, gradient boosting, and hybrid deep learning architectures effectively capture nonlinear temporal dependencies and seasonal variations, leading to improved grid scheduling, pricing strategies, and system stability [10], [13].

Renewable energy forecasting is another key application, as solar and wind power introduce significant variability and uncertainty. ML models utilize meteorological data, sensor measurements, and satellite imagery to predict energy output, with deep learning architectures such as CNN–LSTM models demonstrating strong performance in modeling cloud movements, wind speed fluctuations, and irradiance patterns [9], [10].

ML is also extensively used for fault detection and grid stability assessment. By learning subtle deviations in system behavior, ML-based classifiers and anomaly detection techniques outperform traditional threshold-based methods and help prevent cascading failures. Reinforcement Learning (RL) has further been explored for autonomous grid reconfiguration and real-time corrective actions [12], [43]. Additionally, ML techniques support energy theft detection and cyber-attack mitigation by analyzing fine-grained consumption data from smart meters to identify irregular or malicious patterns [14], [44], [45].

B. ML Applications in Industrial IoT and Industry 4.0

In Industrial IoT and Industry 4.0 environments, ML enables predictive intelligence, automation, and optimized production [6], [17]. Predictive maintenance is a dominant application, where ML models analyze vibration signals, temperature readings, acoustic emissions, and sensor logs to estimate equipment remaining useful life and detect early signs of degradation, thereby reducing downtime and maintenance costs [16], [18].

ML-based computer vision systems support automated quality inspection by identifying defects and ensuring compliance with manufacturing standards. ML also plays a key role in anomaly detection and cyber-physical process monitoring, allowing industrial systems to operate autonomously while preventing hazardous conditions [19], [33], [40], [41]. Furthermore, ML-enhanced digital twins enable accurate state estimation, predictive simulation, and adaptive control, allowing models to be tested in virtual environments before deployment in real-world operations [15], [19].

C. ML Applications in Smart Agriculture

Smart Agriculture leverages CPS and ML to enable precision farming and sustainable food production [22], [24]. ML models support crop yield prediction by integrating historical yield data, weather conditions, soil parameters, and satellite imagery, with ensemble and deep learning approaches providing high predictive accuracy [25], [46].

Computer vision–based ML techniques enable early disease detection and plant health monitoring, allowing timely interventions and reducing large-scale agricultural losses [21], [22]. ML is also applied to soil and irrigation management, where sensor data is used to optimize irrigation schedules and nutrient application through adaptive control strategies [23], [24]. Finally, autonomous farming systems integrate ML with robotics and drone-based imaging to support automated harvesting, spraying, crop monitoring, and efficient navigation in complex agricultural environments [22], [46].

ML-Enabled Security in Cyber-Physical Systems

Cyber-Physical Systems (CPS) are increasingly exposed to sophisticated cyber threats due to their extensive connectivity, heterogeneous components, and real-time operational constraints. Traditional signature-based and rule-driven security mechanisms are often inadequate for detecting novel, evolving, and stealthy attacks in such dynamic environments. As a result, Machine Learning (ML) has emerged as a critical enabler of intelligent, adaptive, and autonomous security mechanisms capable of enhancing CPS resilience and trustworthiness [4], [45].

ML-driven security solutions analyze high-dimensional and multimodal data generated by sensors, controllers, network traffic, and system logs to identify behavioral deviations, predict malicious activities, and support rapid mitigation strategies. By enabling continuous learning, contextual awareness, and adaptive decision-making, ML significantly strengthens the robustness and reliability of CPS against cyber and cyber-physical attacks [20], [40].

A. Role of ML in Enhancing CPS Security

ML enhances CPS security through four major functional capabilities. Anomaly detection techniques identify deviations from normal operational behavior, enabling early detection of intrusions, sensor spoofing, communication anomalies, and system malfunctions using models such as autoencoders, clustering algorithms, and one-class SVMs.

Intrusion Detection Systems (IDS) based on ML outperform traditional rule-based approaches by learning complex attack patterns and network behaviors. Deep learning models, including CNNs and LSTMs, have demonstrated strong performance in detecting DoS, false-data injection, replay, and jamming attacks [41].

ML is also applied to threat prediction and risk assessment, where predictive models evaluate system vulnerabilities and forecast potential attack paths. Reinforcement learning (RL) further supports adaptive defense strategies by dynamically optimizing responses based on evolving system states. Automated response and mitigation mechanisms leverage RL-based control policies to autonomously reconfigure CPS components during attacks, such as isolating compromised nodes or modifying network routes [50].

B. ML Techniques Used for CPS Security

A wide range of ML paradigms is employed in CPS security, depending on system requirements and threat models. Supervised learning algorithms are commonly used for classifying known attack types, while unsupervised learning techniques play a crucial role in detecting zero-day attacks and unexpected behaviors without labeled data. Deep learning models process high-dimensional network and sensor data to capture spatial and temporal attack patterns, while Generative Adversarial Networks (GANs) are used to simulate attack scenarios and improve model robustness. Reinforcement learning enables adaptive and distributed defense strategies under uncertain and dynamic conditions. Federated Learning (FL) further supports privacy-preserving security analytics by allowing collaborative model training without sharing raw data across CPS nodes [38], [39].

C. Security Threats Addressed by ML in CPS

ML-enabled security solutions address several critical CPS threats, including false data injection attacks, replay and spoofing attacks, denial-of-service attacks, malware propagation, and insider threats. By analyzing behavioral patterns and temporal dependencies, ML models can identify malicious activities in real time and mitigate their impact across CPS domains such as smart grids and industrial control systems [14], [41], [45].

D. Challenges and Emerging Trends

Despite its advantages, ML-based CPS security faces challenges related to data quality, adversarial manipulation, real-time constraints, interpretability, and resource limitations at the edge [38], [39], [50]. Emerging trends include Explainable AI for transparent security decisions, lightweight ML models for embedded devices, adversarially robust learning, blockchain-assisted secure data sharing, and multi-agent RL for cooperative distributed defense strategies [29], [50].

Deployment Considerations for Machine Learning in CPS: Edge, Fog, and Cloud Paradigms

The deployment of Machine Learning capabilities within Cyber-Physical Systems involves a multilayered computational hierarchy that must satisfy stringent requirements for latency, reliability, energy efficiency, scalability, and security. CPS domains such as smart grids, industrial automation, and precision agriculture generate massive, continuous streams of sensor data that must be processed in real time to support safety-critical decision-making. While cloud platforms offer virtually unlimited storage and computational power, their centralized nature is often incompatible with CPS workloads that demand ultra-low latency and high resilience. Consequently, CPS research has increasingly shifted toward distributed ML deployment across edge, fog, and cloud layers, each providing unique advantages and trade-offs [26], [27], [28].

A. Edge-Level Machine Learning [26], [27] [28], [30]

Edge computing positions data processing directly on or near physical devices such as sensors, embedded controllers, and microprocessors. Deploying ML models at the edge enables immediate response to environmental stimuli, making it suitable for industrial robotics, autonomous energy management, and agricultural field monitoring.

Edge ML reduces communication overhead by eliminating the need to transmit raw data to remote servers, thereby lowering bandwidth consumption and enhancing privacy. However, edge devices often possess limited memory, computational capacity, and energy resources. This necessitates the adoption of lightweight ML approaches such as TinyML, model pruning, quantization, and hardware accelerators. Ensuring robustness of edge-deployed ML models against environmental noise, intermittent connectivity, and resource variability remains an active research direction.

B. Fog-Level Machine Learning [26], [28] , [29], [42]

Fog computing introduces an intermediate layer between edge devices and centralized cloud infrastructure. This layer comprises distributed micro-datacenters, gateways, and network nodes capable of performing mid-complexity ML tasks. Fog ML is advantageous for CPS scenarios requiring a balance between low latency and higher computational resources than those available at the edge. In smart grids, fog nodes can execute localized load prediction or anomaly detection for specific substations, enabling coordinated distributed intelligence.

Fog infrastructures support collaborative ML paradigms such as federated learning and edge–fog co-training, where models are updated by aggregating insights from multiple devices while preserving data locality. Nevertheless, fog-based deployments must address challenges related to heterogeneous platforms, dynamic workload allocation, network congestion, and secure orchestration of distributed ML pipelines.

C. Cloud-Level Machine Learning [15], [27], [26], [45].

Cloud platforms provide substantial computational and storage resources, enabling the development and training of high-complexity ML models such as deep neural networks, transformers, and large-scale reinforcement learning policies. Within CPS, the cloud is particularly suited for centralized analytics, global optimization tasks, long-term forecasting, digital twin simulations, and model lifecycle management.

Despite these capabilities, reliance on cloud computing introduces latency, bandwidth limitations, and vulnerabilities associated with network interruptions. Furthermore, transmitting large sensor datasets to remote servers may increase exposure to cyber threats and raise privacy concerns. As a result, cloud ML is most effective when complemented by distributed intelligence at edge and fog layers, forming a hierarchical CPS architecture that supports real-time operations while enabling high-level predictive analytics.

D. Hybrid Edge–Fog–Cloud ML Architectures [26], [28], [29], [42]

Modern CPS increasingly adopt hybrid ML deployments that leverage the complementary strengths of all three computational layers. In such systems, edge devices perform initial inference or feature extraction, fog nodes execute intermediate analytics and model aggregation, and cloud servers handle complex training or global optimization.

This collaborative architecture enhances scalability, reduces communication load, and improves resilience by enabling fallback mechanisms when specific layers fail. Research in hierarchical ML frameworks has demonstrated improvements in energy efficiency, latency reduction, and adaptability across diverse CPS domains. However, designing optimal partitioning strategies, ensuring synchronization among distributed components, and mitigating cascading failures remain key challenges.

E. Trade-Offs and Design Principles [26], [28]

Effective ML deployment in CPS requires consideration of several trade-offs:

Latency vs. Model Complexity:

Lower-latency applications favor simplified edge models, whereas accuracy-intensive tasks may require cloud or fog execution.

Bandwidth vs. Local Processing:

Extensive local computation reduces communication load but may exceed device capabilities.

Energy Consumption vs. Real-Time Responsiveness:

ML inference at the edge must balance energy efficiency with the need for rapid control responses.

Security vs. Computational Overhead:

Implementing robust encryption, authentication, and anomaly detection increases computational demands across layers.

Scalability vs. Coordinated Control:

Distributed architectures scale efficiently but require sophisticated coordination to maintain system stability.

F. Emerging Trends in CPS ML Deployment [30], [35]

Recent advancements point toward more intelligent and adaptive deployment strategies, including dynamic model migration, on-device continual learning, neuromorphic accelerators, swarm intelligence architectures, and decentralized reinforcement learning. These innovations aim to enable CPS that autonomously redistribute computational workloads, adapt to environmental variations, and evolve with minimal human intervention.

CONCLUSION

Cyber-Physical Systems (CPS) are rapidly transforming critical infrastructures by tightly integrating sensing, computation, communication, and control capabilities. As these systems continue to grow in scale, complexity, and autonomy, traditional analytical and rule-based methods become increasingly inadequate for managing the dynamic behavior, uncertainty, and data-intensive nature of modern CPS environments. In this context, Machine Learning (ML) has emerged as a foundational enabler for realizing intelligent, adaptive, and resilient CPS operations.

This review has presented a comprehensive synthesis of ML techniques and their applications across major CPS domains, including Smart Grids, Industrial IoT and Industry 4.0, and Smart Agriculture. The analysis demonstrates that ML significantly enhances CPS functionality by enabling accurate forecasting, robust anomaly detection, predictive maintenance, real-time optimization, and improved decision-making under uncertain conditions. Advanced deep learning architectures and reinforcement learning frameworks, in particular, have shown strong potential in supporting autonomous control and high-dimensional data processing within CPS ecosystems.

Despite these advances, the integration of ML into CPS remains challenging. Constraints related to limited computational resources at the edge, strict latency requirements, safety and reliability demands, data heterogeneity, and exposure to adversarial threats continue to impede large-scale deployment. Moreover, the need for explainable and trustworthy ML models is especially critical in mission- and safety-critical CPS applications, where transparency and verifiable system behavior are essential for operational trust and regulatory compliance.

Looking ahead, emerging research directions such as TinyML for resource-constrained devices, federated learning for privacy-preserving distributed intelligence, multimodal learning for heterogeneous data fusion, and self-healing CPS architectures offer promising pathways forward. Addressing these challenges through interdisciplinary collaboration across machine learning, control systems, networking, cybersecurity, and domain engineering will be vital. Ultimately, ML-enabled CPS are poised to play a transformative role in advancing sustainable, intelligent, and resilient future infrastructures.

REFERENCES

1. E. A. Lee, “Cyber Physical Systems: Design Challenges,” Proc. IEEE Int. Symp. Object Oriented Real-Time Distributed Computing (ISORC), 2008.
2. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, “Cyber-Physical Systems: The Next Computing Revolution,” Proc. 47th ACM/IEEE Design Automation Conf. (DAC), 2010.
3. J. Stankovic, “Research Directions for the Internet of Things,” IEEE Internet Things J., vol. 1, no. 1, pp. 3–9, 2014.
4. M. Wolf, D. Serpanos, “Safety and Security in Cyber-Physical Systems and Internet-of-Things Systems,” Proc. IEEE, vol. 106, no. 1, pp. 9–20, 2018.
5. W. He, G. Yan, and L. Da Xu, “Developing Cyber-Physical Systems based on Cybernetics,” IEEE Trans. Ind. Informat., vol. 13, no. 2, pp. 1048–1059, 2017.
6. H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, “The Industrial Internet of Things (IIoT): An Analysis Framework,” Comput. Ind., vol. 101, pp. 1–12, 2018.
7. P. Siano, “Demand Response and Smart Grids—A Survey,” Renewable Sustainable Energy Rev., vol. 30, pp. 461–478, 2014.
8. Y. Wang, Q. Chen, T. Hong, and C. Kang, “Review of Smart Meter Data Analytics: Applications, Methodologies, and Challenges,” IEEE Trans. Smart Grid, vol. 10, no. 3, pp. 3125–3148, 2019.
9. K. Zhou, C. Fu, and S. Yang, “Big Data Driven Smart Energy Management: From Big Data to Big Insights,” Renewable Sustainable Energy Rev., vol. 56, 2016.
10. T. Hong and P. Pinson, “Probabilistic Energy Forecasting: State of the Art,” IEEE Trans. Smart Grid, vol. 5, no. 5, pp. 1461–1470, 2014.
11. E. Mocanu et al., “On-line Building Energy Optimization Using Deep Reinforcement Learning,” IEEE Trans. Smart Grid, vol. 10, no. 4, 2019.
12. S. Bhela et al., “Fault Classification and Location in Power Distribution Networks Using Machine Learning,” IEEE Trans. Smart Grid, vol. 11, no. 3, 2020.
13. Y. Zhang, L. Wang, “Machine Learning Approaches for Smart Grid Load Forecasting: A Survey,” IEEE

Access, vol. 7, pp. 10155–10166, 2019.
14. H. Zhong et al., "Energy Theft Detection in Smart Grids Using ML," IEEE Trans. Ind. Informat., vol. 18, no. 2, pp. 1351–1361, 2022.
15. Q. Qi and F. Tao, "Digital Twin and Big Data Towards Smart Manufacturing," IEEE Access, vol. 6, pp. 70504–70514, 2018.
16. S. Yin, et al., "Data-Driven Monitoring and Diagnosis for Industrial Systems: A Review," IEEE Trans. Ind. Electron., vol. 61, no. 7, 2014.
17. J. Lee, B. Bagheri, H. Kao, "A Cyber-Physical Systems Architecture for Industry 4.0-based Manufacturing Systems," Manufacturing Letters, vol. 3, 2015.
18. A. Jain, S. Kumar, "Predictive Maintenance Using Sensor Data Analytics," IEEE Sensors J., vol. 21, no. 4, 2021.
19. F. Tao, Q. Qi, A. Liu, and A. Kusiak, "Data-Driven Smart Manufacturing," J. Manuf. Syst., vol. 48, 2018.
20. M. A. Khan and K. Salah, "IoT Security: Review, Blockchain Solutions, and Open Challenges," Future Gener. Comput. Syst., 2018.
21. S. Mohanty, D. Hughes, "Using Deep Learning for Plant Disease Detection," IEEE Access, 2016.
22. A. Kamilaris, F. Prenafeta-Boldú, "Deep Learning in Agriculture: A Survey," Comp. Electron. Agric., vol. 147, 2018.
23. M. Sharada, P. Singh, "AI-Based Smart Irrigation Systems," IEEE Trans. Autom. Sci. Eng., vol. 18, 2021.
24. A. Chlingaryan, S. Sukkarieh, "Machine Learning for Precision Agriculture," Comp. Electron. Agric., 2018.
25. J. Zhang, et al., "Soil Moisture Estimation Using Ensemble ML Models," Agric. Water Manag., 2021.
26. W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge Computing: Vision and Challenges," IEEE Internet Things J., vol. 3, no. 5, 2016.
27. M. Satyanarayanan, "The Emergence of Edge Computing," Computer, vol. 50, no. 1, pp. 30–39, 2017.
28. Z. Zhou et al., "Edge Intelligence: State-of-the-Art and Future Trends," Proc. IEEE, vol. 107, no. 8, pp. 1655–1674, 2019.
29. P. Kairouz et al., "Advances and Open Problems in Federated Learning," Found. Trends Mach. Learn., 2021.
30. H. Ghods, "A Review of TinyML," ACM Trans. Embeded Comput. Syst., 2022.
31. G. E. Hinton et al., "Deep Learning," Nature, vol. 521, pp. 436–444, 2015.
32. Y. LeCun, Y. Bengio, and G. Hinton, "Deep Learning," Nature, 2015.
33. A. Krizhevsky, I. Sutskever, and G. Hinton, "ImageNet Classification with Deep CNNs," NIPS, 2012.
34. S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory," Neural Comput., 1997.
35. D. Silver et al., "Mastering Control with Deep Reinforcement Learning," Nature, 2016.
36. V. Vapnik, "The Nature of Statistical Learning Theory," Springer, 1995.
37. L. Breiman, "Random Forests," Machine Learning, vol. 45, 2001.
38. I. Goodfellow et al., "Explaining and Harnessing Adversarial Examples," ICLR, 2015.
39. X. Yuan et al., "Adversarial Attacks and Defenses in Deep Learning," IEEE Trans. Neural Netw. Learn. Syst., 2019.
40. F. Amiri et al., "Anomaly Detection in Cyber-Physical Systems," IEEE Internet Things J., 2019.
41. T. Yang, "Intrusion Detection for Industrial CPS," IEEE Trans. Ind. Informat., 2020.
42. M. Liu, X. Li, "Security of Distributed CPS Architectures," IEEE Commun. Surveys Tuts., 2021.
43. G. Ramos et al., "Stability Prediction in Smart Grids," IEEE Access, 2020.
44. M. Rahman, "Energy Theft Detection Using ML," IEEE PES, 2020.
45. X. Fang et al., "Smart Grid Cybersecurity: A Survey," IEEE Commun. Surveys Tuts., 2012.
46. V. Sharma, R. Kumar, "Agriculture IoT with ML: A Survey," Sensors, 2020.
47. Q. Yang et al., "Transfer Learning for Smart Systems," IEEE TKDE, 2020.
48. J. Gama et al., "A Survey on Concept Drift," IEEE TKDE, 2014.
49. C. Szegedy et al., "Intriguing Properties of Neural Networks," ICLR, 2014.
50. F. Kang, L. Xu, "Secure Machine Learning for CPS: A Review," ACM Comput. Surveys, 2021.