

Review

AI-Based Autonomous Security for Cyber–Physical Systems 2.0 in IoT Ecosystems—A Narrative Review

Izabela Rojek , Piotr Kotlarz and Dariusz Mikołajewski * 

Faculty of Computer Science, Kazimierz Wielki University, 30 Chodkiewicza St., 85-064 Bydgoszcz, Poland; izabela.rojek@ukw.edu.pl (I.R.); piotr.kotlarz@ukw.edu.pl (P.K.)

* Correspondence: dariusz.mikolajewski@ukw.edu.pl

Abstract

This narrative review examines the evolving landscape of AI-based security in Cyber–Physical Systems 2.0 (CPS 2.0) within the context of AI-driven autonomous cybersecurity solutions for the Internet of Things (IoT). This article presents a narrative review, supported by a structured literature search inspired by the PRISMA 2020 project and descriptive publication statistics. It combines transparent study selection with qualitative conceptual synthesis, rather than a formal systematic review or bibliometric analysis. CPS 2.0 represents a new generation of interconnected systems that tightly integrate physical processes with intelligent computational components, enabling increased autonomy and operational efficiency. However, this growing complexity introduces advanced security threats and privacy challenges that traditional centralized security frameworks are ill-equipped to address due to limitations in scalability, latency, and data sensitivity. The paper explores how artificial intelligence (AI), machine learning (ML), and generative AI (GenAI) enhance real-time threat detection, prediction, and response in distributed environments. It highlights the role of edge computing in decentralizing intelligence, thereby reducing latency and limiting exposure of sensitive data. Additionally, federated learning (FL) is discussed as a privacy-preserving paradigm that enables collaborative model training across distributed nodes without sharing raw data. The integration of GenAI, FL, and edge computing is presented as a synergistic approach that enables adaptive, context-aware, and proactive defense mechanisms against dynamic and evolving cyber threats. The review further analyzes architectural frameworks, key advantages, and inherent vulnerabilities of CPS 2.0, along with mitigation strategies and real-world applications, particularly in industrial control systems. By synthesizing current advancements and challenges, this work provides a comprehensive roadmap for designing resilient, scalable, and privacy-aware CPS infrastructures. The findings contribute to the development of secure and intelligent systems aligned with the future demands of Industry 4.0, 5.0, and beyond.



Academic Editor: Priyadarsi Nanda

Received: 21 June 2026

Revised: 22 July 2026

Accepted: 27 July 2026

Published: 28 July 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

Keywords: industry; automation; artificial intelligence; cyber–physical systems; human-centric approach; privacy; security; AI-driven cybersecurity; IoT security; explainable AI

1. Introduction

Cyber–Physical Systems 2.0 (CPS 2.0) evolved from first-generation CPS architectures, which primarily integrated embedded systems with physical processes for monitoring and control [1]. While CPS 1.0 enabled significant automation in areas such as manufacturing, transportation, and healthcare, it lacked the intelligence and adaptability required in highly dynamic IoT environments. The convergence of artificial intelligence (AI), Internet

of Things (IoT) technologies, edge computing, and advanced communication networks fueled the transformation toward CPS 2.0. In this new paradigm, systems are capable of autonomous learning, predictive analytics, and real-time decision-making, improving both operational efficiency and security [2]. AI-based autonomous security mechanisms play a key role in CPS 2.0, continuously detecting, analyzing, and responding to cyberthreats across interconnected devices and physical infrastructures. The implementation of 5G technology and low-latency communications further supports distributed intelligence, enabling secure and seamless interaction between heterogeneous IoT components. Unlike traditional security approaches, CPS 2.0 leverages self-adaptive defense strategies that dynamically adapt to changing threats and system conditions [3]. Human decision-making capabilities remain crucial, ensuring that autonomous security decisions are supervised and verified when necessary to maintain security and trust. Furthermore, interoperability, standardization, and energy efficiency are fundamental features that facilitate secure collaboration across diverse CPS and IoT ecosystems (Figure 1) [4]. Therefore, CPS 2.0 represents a significant step forward towards resilient, intelligent, and autonomous cyber-physical environments capable of addressing the growing security challenges of modern connected systems.

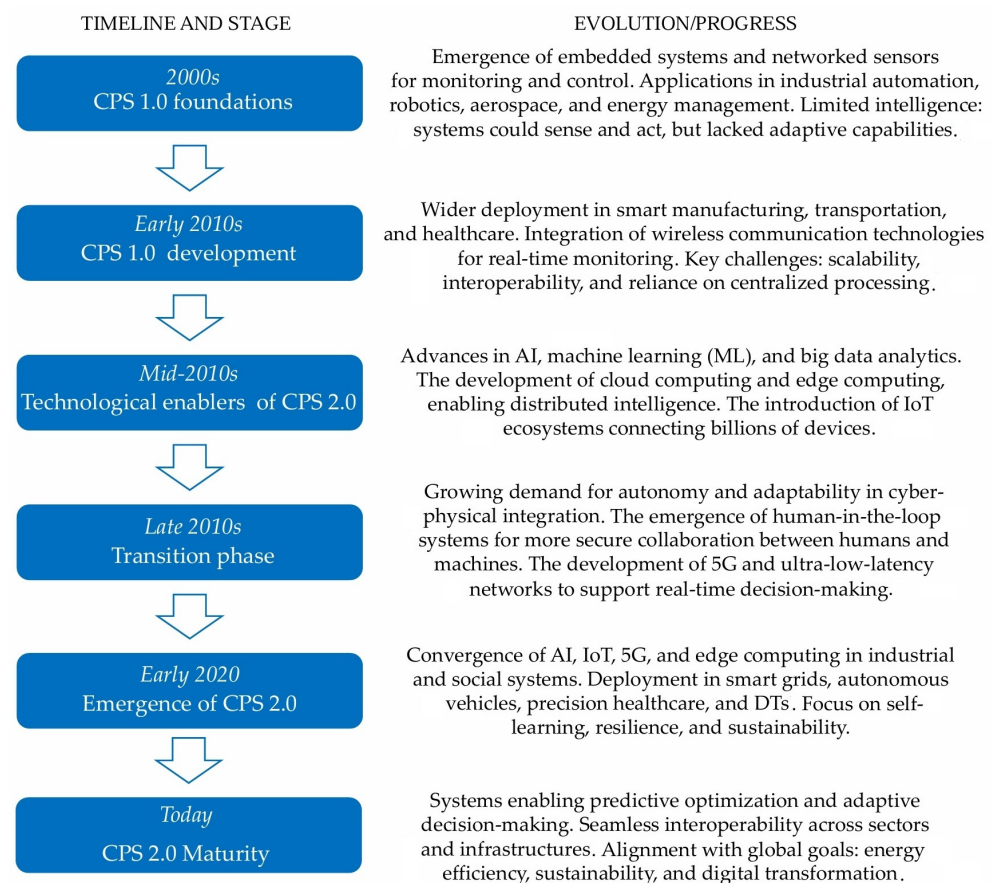


Figure 1. Evolution from CPS 1.0 to CPS 2.0 (own elaboration based on [5–14]).

1.1. From Conventional CPS to CPS 2.0: Conceptual Evolution and Defining Characteristics

CPSs have evolved significantly over the past two decades, driven by rapid advances in AI, IoT, edge computing, cloud-native architectures, and distributed data analytics. Conventional CPSs were originally conceived as tightly integrated systems combining sensors, computation, communication, and control to monitor and control physical processes in fields such as industrial automation, transportation, healthcare, and energy systems. Their primary goal was to achieve reliable, deterministic, and real-time interaction be-

tween cyber and physical components through predefined control logic and centralized supervision architectures [5]. While these characteristics remain fundamental, the increasing scale, heterogeneity, and connectivity of modern IoT ecosystems have exposed the limitations of traditional CPS architectures. Contemporary deployments often involve thousands or even millions of interconnected devices generating continuous streams of data, operating in highly dynamic environments, and facing increasingly sophisticated cyberthreats. Conventional centralized security mechanisms and static, rule-based control strategies often struggle to deliver the scalability, adaptability, and resilience required in these environments [6]. In this review, the term CPS 2.0 is used to describe the next stage in the evolution of cyber-physical systems, rather than a completely new technological paradigm. CPS 2.0 extends the traditional CPS architecture by embedding intelligence, autonomy, distributed computing, and adaptive cybersecurity as internal architectural components rather than optional add-ons. Therefore, CPS 2.0 should be understood as an architectural evolution that reflects the convergence of AI, edge intelligence, FL, DTs, cloud-edge collaboration, and autonomous decision-making.

A hallmark of CPS 2.0 is the shift from automation to autonomy. Conventional CPSs primarily implement predefined control strategies developed by experts. Although adaptive controllers are possible, operational decisions are typically made based on deterministic algorithms with limited learning capabilities. In contrast, CPS 2.0 continuously acquires operational knowledge from distributed data sources, leveraging AI and ML models capable of learning, adapting, predicting, and autonomously optimizing. These capabilities allow the system to dynamically adapt its behavior in response to changing environmental conditions, hardware degradation, or emerging cyberthreats, without requiring extensive human intervention. Another fundamental difference concerns the computational architecture. Traditional CPSs often rely on centralized cloud platforms or supervisory control systems for data aggregation and decision-making [7]. With the continued growth of IoT deployments, centralized processing introduces communication delays, bandwidth constraints, single points of failure, and increased privacy risks. CPS 2.0 addresses these challenges by adopting hierarchical cloud-edge architectures, where intelligence is distributed across edge devices, fog nodes, and cloud services. Processing data closer to its source enables low-latency decision-making, improves system resilience, and reduces unnecessary transmission of sensitive information. The security paradigm is also undergoing a significant transformation. Conventional CPS defenses rely primarily on perimeter protection, signature-based intrusion detection, predefined security policies, and periodic software updates [8]. These approaches are increasingly insufficient against advanced attacks that exploit zero-day vulnerabilities, advanced persistent threats, and AI-assisted attack strategies. CPS 2.0 introduces autonomous cybersecurity mechanisms that continuously monitor system behavior, detect anomalies using AI, predict potential attack scenarios, and automatically initiate appropriate risk mitigation strategies. Security, therefore, becomes a continuous, adaptive, and self-improving process rather than a static defense layer. Privacy-preserving intelligence is another key differentiator [9]. Traditional machine learning approaches typically require centralized aggregation of operational data for model training, raising concerns about confidentiality, regulatory compliance, and data sharing within organizations. CPS 2.0 increasingly leverages FL technology, enabling distributed devices to collaboratively train global models without transferring raw data outside their local environments. This approach significantly enhances privacy while maintaining high-quality predictions across geographically distributed infrastructures [10]. Furthermore, CPS 2.0 incorporates complementary technologies largely lacking in previous generations of CPSs. Digital twins enable continuous synchronization between physical assets and virtual representations, supporting predictive maintenance, operational

optimization, and security assessment. GenAI extends traditional machine learning by enabling automated threat analysis, vulnerability assessment, attack simulation, and intelligent security support [11]. Combined with edge computing and federated learning, these technologies create an adaptive ecosystem capable of responding to rapidly changing operational and cybersecurity requirements [12].

It is important to emphasize that the mere presence of AI does not automatically qualify a system as CPS 2.0. Many existing CPS implementations integrate isolated ML models for specific tasks, such as predictive maintenance or anomaly detection, while maintaining centralized architectures and conventional security mechanisms [13]. In this review, a system is considered CPS 2.0 only if intelligence, distributed computing, autonomous decision-making, and adaptive cybersecurity are integrated as fundamental architectural principles that jointly govern system operation. Therefore, this review adopts the CPS 2.0 concept as a comprehensive framework for next-generation intelligent cyber–physical ecosystems supporting Industry 4.0, Industry 5.0, smart manufacturing, smart transportation, healthcare, and critical infrastructure. The combination of AI-driven autonomy, distributed intelligence, privacy-preserving collaborative learning, and proactive cybersecurity provides the foundation for resilient, scalable, and trustworthy cyber–physical infrastructures capable of addressing the increasingly complex operational and security challenges of future IoT environments (Table 1) [14].

Table 1. Comparison between Conventional CPS and CPS 2.0.

Aspect	Conventional CPS	CPS 2.0
Primary objective	Monitoring and control of physical processes	Autonomous, intelligent, and resilient operation of interconnected cyber–physical ecosystems
System intelligence	Rule-based or deterministic control	AI-driven adaptive intelligence with continuous learning
Decision-making	Centralized or supervisory	Distributed, autonomous, and context-aware
Learning capability	Limited or offline model updates	Continuous online learning and adaptation using AI/ML
Computing architecture	Centralized cloud or control center	Cloud-edge-fog collaborative architecture
Data processing	Predominantly centralized	Distributed processing at edge, fog, and cloud
Scalability	Moderate; limited by centralized infrastructure	High scalability through decentralized intelligence
IoT integration	Connected devices with predefined functionality	Highly heterogeneous, dynamically orchestrated IoT ecosystems
Security model	Perimeter defense, rule-based IDS, signature detection	AI-driven autonomous cybersecurity with predictive threat detection and automated response
Threat response	Manual or semi-automatic	Autonomous, adaptive, and real-time

Table 1. *Cont.*

Aspect	Conventional CPS	CPS 2.0
Privacy protection	Centralized data collection	Federated learning and privacy-preserving distributed intelligence
Communication model	Primarily cloud-centric	Edge-cloud collaborative communication
DTs	Optional or limited use	Integrated for monitoring, prediction, simulation, and resilience
GenAI	Generally absent	Supports threat analysis, vulnerability assessment, automated reasoning, and security assistance
Human involvement	Human-in-the-loop for supervision and decision-making	Human-on-the-loop with autonomous operational support
System resilience	Fault tolerance through redundancy	AI-enhanced self-adaptation, self-healing, and predictive resilience
Typical applications	Industrial automation, Supervisory Control and Data Acquisition (SCADA), process control	Industry 4.0/5.0, smart factories, autonomous transportation, smart grids, intelligent healthcare, critical infrastructure
Representative technologies	Programmable Logic Controllers (PLCs), SCADA, sensor networks, cloud services	AI/ML, GenAI, FL, Edge/Fog Computing, DTs, Zero-Trust Security

1.2. Challenges

To date, CPS 2.0 security research remains fragmented, with limited integration of AI, edge computing, FL, and GenAI within a unified security framework. Traditional, centralized cybersecurity architectures are insufficiently equipped to address the scalability, latency, and privacy requirements of highly distributed, IoT-enabled CPS 2.0 environments. Comprehensive research examining how autonomous AI-based security mechanisms can provide comprehensive protection in heterogeneous CPS 2.0 infrastructures is lacking. The current literature offers limited analysis of the synergistic interactions between FL, edge intelligence, and GenAI in adaptive cyber defense. Insufficient attention has been paid to the vulnerabilities and security threats posed by AI-enabled CPS 2.0 architectures themselves, including model manipulation, adversarial attacks, and trust management issues. There is a significant research gap in developing holistic design guidelines and architectural plans aimed at creating resilient, privacy-preserving, and self-adaptive CPS 2.0 ecosystems for future industrial environments.

This article provides a comprehensive narrative review that consolidates the latest advances in AI-based autonomous security for CPS 2.0 in IoT ecosystems within a single analytical framework. It introduces a multidisciplinary perspective, examining the combined role of AI/ML, GenAI, edge computing, and FL in securing distributed cyber–physical environments. The review highlights the synergistic integration of these components as a foundation for context-aware, privacy-preserving, and proactive cybersecurity mechanisms. It systematically analyzes both the benefits and inherent gaps in CPS 2.0 architecture, offering a balanced assessment of emerging opportunities and threats. The article con-

tributes practical insights by discussing risk mitigation strategies, architectural patterns, and real-world applications, particularly in industrial control systems and intelligent IoT infrastructures. By combining current knowledge with future challenges, the study proposes a roadmap to develop secure, intelligent, scalable and resilient CPS 2.0 systems, adapted to the evolving requirements of Industry 4.0, Industry 5.0 and the future paradigms of Industry 6.0.

The aim of this paper is to examine the security challenges, vulnerabilities, and emerging cyberthreats impacting CPS 2.0 within interconnected IoT ecosystems. Particular attention is paid to the role of autonomous security mechanisms based on AI in detecting, predicting, and mitigating cyberattacks in real time. The paper further assesses the potential of advanced technologies, including edge computing, AI, GenAI, and FL, to enhance system resilience, protect privacy, and adaptively respond to threats. By examining these technologies in the context of critical infrastructures, the study highlights their contribution to securing distributed, intelligent, and highly connected CPS 2.0 environments while supporting autonomous and resilient system operation. The additional aim of the study is to apply a conceptual framework based on answers to the following research questions (RQs):

- RQ1: What AI-based approaches to autonomous security have been proposed and implemented in CPS 2.0 in IoT ecosystems?
- RQ2: What are the main benefits, challenges, and limitations of AI-based autonomous security solutions in CPS 2.0 environments?
- RQ3: How do emerging AI techniques contribute to autonomous threat detection, mitigation, and resilience in IoT-based CPS 2.0?
- RQ4: What are the research gaps and future directions for AI-based autonomous security in CPS 2.0 and IoT ecosystems?

RQs were developed to identify leading research groups and influential authors, examine prevailing research themes, and analyze the contributions of countries and institutions within the field. They also aimed to explore collaborative networks and assess the alignment of existing research with the Sustainable Development Goals (SDGs). The overall objective was to map the global scientific landscape of AI-driven security and privacy solutions based on edge computing and FL for CPS 2.0 and IoT ecosystems.

2. Materials and Methods

The primary goal of this paper is to present a narrative review that offers a comprehensive conceptual synthesis of recent advances in AI-based autonomous cybersecurity for CPS 2.0 in IoT ecosystems. We did not intend to conduct a formal systematic literature review or a full bibliometric study. This manuscript is a narrative review, supported by a structured literature search to enhance transparency and reduce selection bias, rather than an exhaustive evidence synthesis. The PRISMA 2020-inspired workflow was used solely as a transparent reporting mechanism for identifying and selecting relevant publications. The review does not claim full adherence to the PRISMA 2020 guidelines for systematic reviews. Quantitative publication statistics are descriptive and are included to illustrate general publication trends and characterize the reviewed literature. They do not constitute a formal bibliometric analysis involving citation networks, co-authorship analysis, bibliographic coupling, or scientific mapping techniques. We clearly separate the literature identification process from the subsequent narrative synthesis and critical discussion, emphasizing that the main contribution of the paper lies in the qualitative integration and interpretation of current research on AI, ML, GenAI, FL, and edge computing to ensure autonomous CPS 2.0 security.

2.1. Data Set

The aim of this paper is not to provide an exhaustive, systematic review of all publications related to AI or IoT, but to present a focused narrative synthesis of representative, high-quality research on AI-based autonomous security mechanisms for CPS 2.0 in IoT ecosystems. Therefore, the literature selection was dictated by relevance to the research scope rather than by maximizing the total number of included publications.

The reviewed publications were selected to cover the main technological aspects of the field, including AI-based threat detection, ML, GenAI, FL, edge computing, DTs, privacy-preserving security mechanisms, and industrial applications of CPSs.

The objective of this bibliometric study was to evaluate the current state of knowledge and identify effective approaches for designing, implementing, and managing AI-based security and privacy mechanisms that leverage edge computing and FL in CPS 2.0. The study sought to support the efficient deployment of these technologies across diverse application domains and operational scales. Although existing research has predominantly concentrated on domain-specific or localized solutions, the broader capabilities of these technologies within interconnected IoT ecosystems remain insufficiently explored, particularly from an interdisciplinary perspective. To address this research gap, a comprehensive bibliometric analysis was conducted on the global scientific literature published between January 2016 and June 2026, providing insights into research trends, emerging themes, and the evolution of AI-driven security and privacy in CPS 2.0 environments.

The proposed framework and RQs offer a comprehensive assessment of contemporary research trends, technological developments, and implementation practices in both academic and industrial settings related to AI-based autonomous security and privacy for CPS 2.0 within IoT ecosystems. Particular emphasis is placed on the application of edge computing and FL as key enablers of distributed intelligence, privacy preservation, and real-time threat detection and response. The findings provide valuable insights for shaping future research directions, integrating complementary security approaches, and improving the resilience and effectiveness of autonomous CPS 2.0 environments through the development of coordinated strategies and roadmaps. Moreover, the bibliometric analysis contributes to the growing body of knowledge on intelligent cybersecurity, supporting evidence-based decision-making and fostering future scientific advancements, technological innovation, and practical deployment of secure, adaptive, and trustworthy cyber-physical infrastructures in response to emerging societal and global challenges.

2.2. Methods

To maintain methodological transparency and analytical consistency, Sections 3 and 4 are structured to clearly separate bibliometric evidence from its subsequent interpretation. The Section 3 presents objective and directly measurable outcomes obtained from the bibliometric analysis, including publication volumes, citation statistics, keyword co-occurrence patterns, collaboration networks, cluster structures, and other quantitative indicators. The Section 4, in turn, focuses on interpreting these findings by identifying thematic research areas, examining the evolution of scientific trends, and evaluating their relevance to AI-based autonomous security and privacy frameworks for CPS 2.0 and IoT ecosystems. Any percentages, comparative indicators, or performance-related measures reported in the study are derived from representative descriptive analyses conducted across the selected bibliographic databases. Given the diversity of data sources, publication types, and reporting methodologies, the study deliberately avoids excessive numerical precision and does not seek to establish causal relationships or produce universally generalizable conclusions. Instead, the findings should be viewed as descriptive indicators of the current state and development of research, reflecting emerging trends while acknowledging varia-

tions in experimental conditions, methodological designs, data availability, and publication practices within the domains of AI-driven cybersecurity, edge computing, FL, and CPS 2.0.

This study utilized four major bibliographic databases—Web of Science (WoS), Scopus, PubMed, and DBLP—chosen for their extensive coverage of scientific, technical, and interdisciplinary research, rich metadata resources, and global representation of scholarly publications (Figure 2). To ensure the relevance and quality of the dataset, the search process was restricted to publications written in English and guided by predefined inclusion and filtering criteria. Each retrieved record was independently evaluated by three reviewers according to established selection guidelines focused on the domains of AI-based autonomous security, privacy preservation, edge computing, FL, and CPS 2.0 within IoT ecosystems. To enhance consistency and minimize selection bias, a publication was only included in the final dataset when at least two of the three reviewers reached agreement regarding its eligibility. Additional relevant studies were identified through backward and forward citation tracking and manual selection of high-relevance publications. This approach reflects the narrative nature of the review and aims to balance thematic focus with comprehensive coverage of the field.

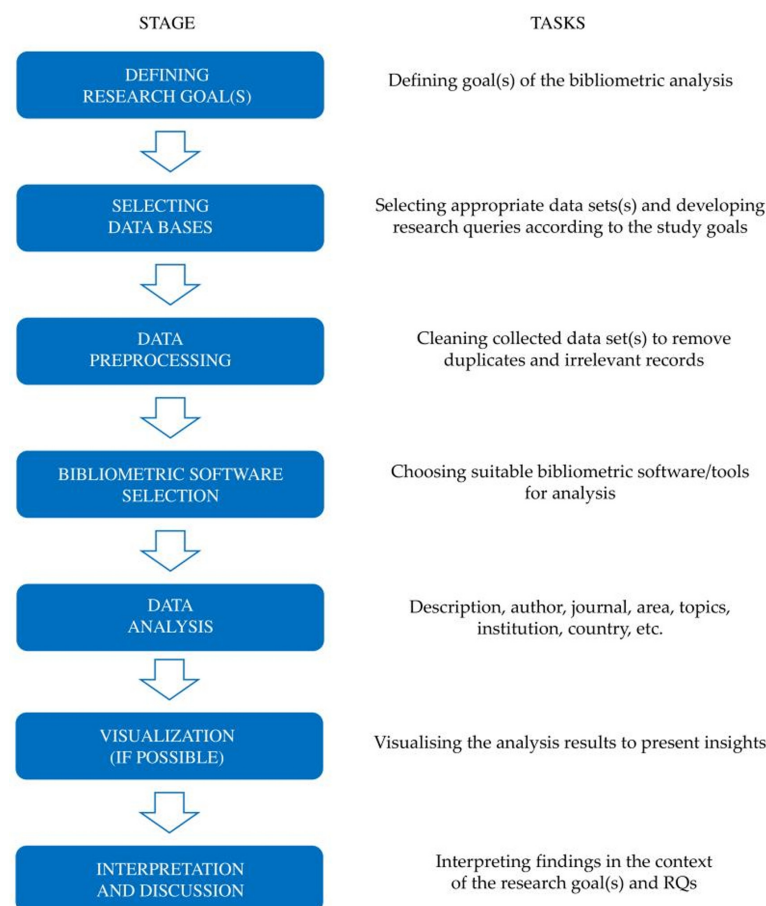


Figure 2. Methodology of bibliometric analysis.

The finalized dataset was systematically examined to identify the principal characteristics of the research landscape, including leading authors, influential institutions and research groups, contributing countries, dominant research themes, and emerging scientific directions. This analysis facilitated the mapping of key concepts and terminology related to AI-based autonomous security, privacy preservation, edge computing, and FL in CPS 2.0 and IoT ecosystems, while also capturing their evolution over time. In addition, temporal analyses were conducted to uncover shifts in research focus, changes in thematic

priorities, and major technological and methodological advancements within the field. Where relevant, longitudinal trends were further explored to identify emerging areas of interest and evolving research agendas. To provide a structured understanding of the domain, publications were grouped into thematic clusters, revealing relationships among research topics and highlighting interdisciplinary connections across cybersecurity, artificial intelligence, distributed computing, and cyber–physical systems.

Regarding eligibility criteria, because the review combined publications retrieved from multiple bibliographic databases (Web of Science, Scopus, PubMed, and DBLP), database-specific search strategies were used to account for differences in indexing policies and search features. For example, Web of Science was searched using the Subject field, Scopus was searched using the Title–Abstract–Keywords fields, while PubMed and DBLP required keyword-based search strategies consistent with their indexing models. These differences were solely intended to maximize the retrieval of potentially relevant publications and should not be interpreted as differences in study selection criteria. After retrieval and duplicate removal, all records were assessed using a common eligibility protocol, regardless of their source database. Publications were included if they addressed AI-based cybersecurity, autonomous security mechanisms, cyber–physical systems (CPS/CPS 2.0), IoT environments, or enabling technologies such as edge computing, FL, or GenAI. Titles and abstracts were initially screened, and then, when relevance could not be determined based on metadata alone, full-text review was conducted. Studies that fell outside the scope of the topic, lacked sufficient technical content, or were not directly related to autonomous cybersecurity in CPSs were excluded. As a result, although database-specific search logic influenced the initial search process, the final literature corpus was generated through a standardized and uniform eligibility assessment, ensuring methodological consistency and comparability across sources.

To ensure the accuracy, consistency, and reliability of the dataset, all retrieved bibliographic records were integrated. Duplicate records were detected through the comparison of titles, Digital Object Identifiers (DOIs), author information, publication years, and other associated metadata. This procedure was complemented by a detailed manual review to address ambiguous cases, including conference proceedings and their subsequently extended journal versions, thereby ensuring appropriate classification and inclusion decisions. Through this combined automated and manual validation process, duplicate and near-duplicate entries were systematically removed prior to the screening stage, enhancing the integrity of the dataset and supporting the robustness of the bibliometric analysis of AI-based autonomous security, privacy preservation, edge computing, and FL in CPS 2.0 and IoT ecosystems.

This study followed ten selected items from the PRISMA 2020 guidelines for bibliographic reviews [15], focusing on essential components such as the study rationale, research objectives, eligibility criteria, data sources, search strategy, study selection, data extraction and collection procedures, synthesis methods, results, and discussion, with detailed descriptions provided in the Supplementary Materials. Bibliometric analyses were performed using analytical tools associated with the Web of Science, Scopus, PubMed, and DBLP databases to ensure wide-ranging and comprehensive literature coverage. This structured methodological framework enhances reproducibility by enabling systematic categorization across key dimensions, including research concepts, thematic areas, authorship, document types, and publication venues. The results are presented in tabular format to support clarity, facilitate interpretation, and enable subsequent analytical processing and visualization.

3. Results

3.1. Data Sources

To improve the precision of the dataset, advanced filtering strategies were applied to restrict the results to English-language publications. In addition, database-specific search functionalities were utilized, including topic-based queries in Web of Science, combined title–abstract–keyword searches in Scopus, and manually curated keyword sets in PubMed and DBLP. These tailored search approaches ensured consistent retrieval of relevant studies across all selected bibliographic sources. The final search string included the most effective terms (“cyber physical system” OR “cyber-physical system” OR CPS) AND (security OR privacy) AND (“autonomy”) (Figure 3).

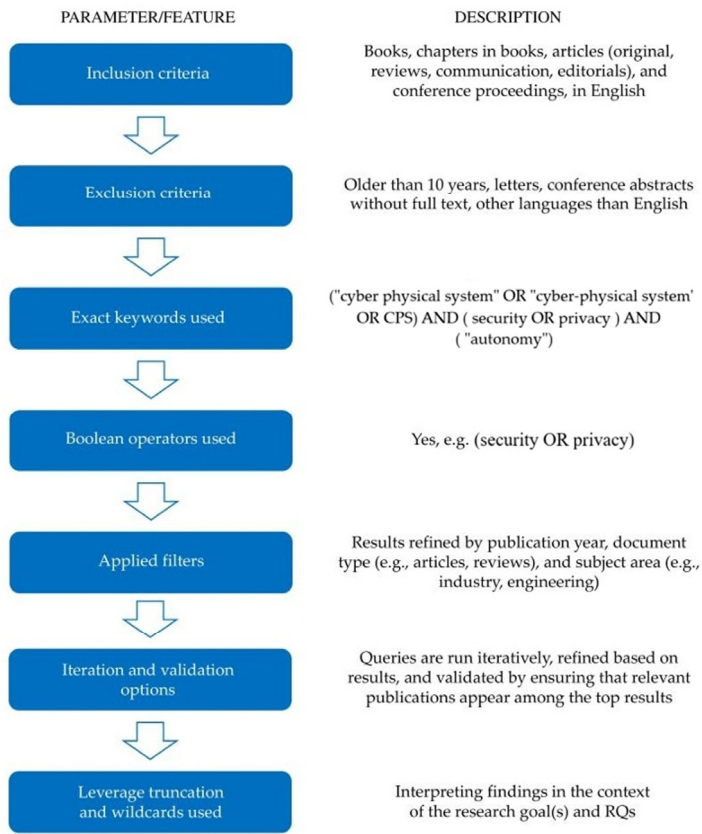


Figure 3. Database search query.

The retrieved publications were subsequently subjected to manual screening to remove irrelevant studies and duplicate records, enabling the determination of the final dataset size (Figure 4).

The PRISMA 2020 flow diagram outlines a structured, stepwise procedure for identifying, screening, evaluating, and ultimately including studies in a systematic review, thereby ensuring methodological rigor and reproducibility. The process started with the identification stage, during which records are gathered from bibliographic databases and other sources, followed by the removal of duplicate entries. In the screening stage, titles and abstracts were evaluated against predefined eligibility criteria, leading to the exclusion of clearly irrelevant studies. The eligibility stage involved a detailed full-text assessment focused on methodological quality, relevance to data collection, and alignment with key topics such as security and system development. The inclusion stage determined the set of studies retained for synthesis and further analysis. Interpretation of the above PRISMA flow diagram enhances transparency by clearly defining the scope of the reviewed literature and providing justification for each exclusion decision.

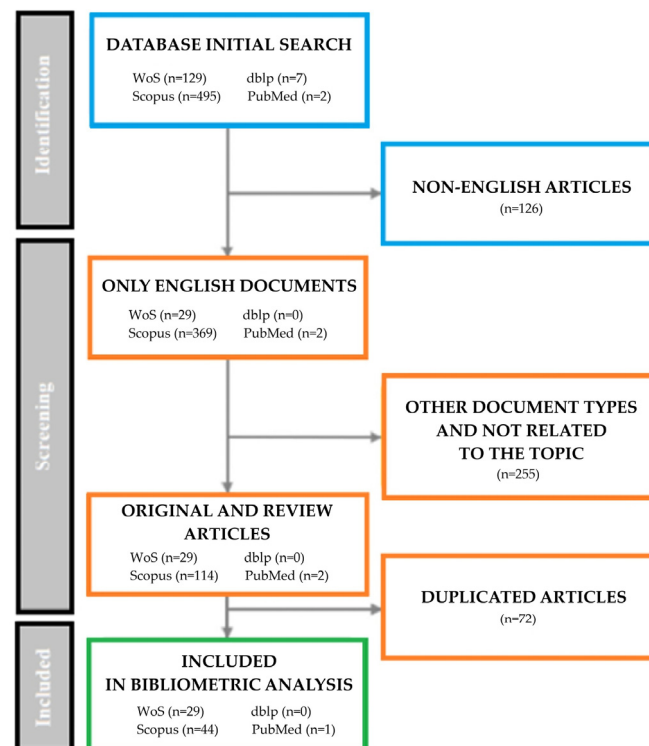


Figure 4. PRISMA 2020 flow diagram.

This article is deliberately structured as a traditional (narrative) review rather than a fully systematic review, applying only selected components of the PRISMA 2020 framework. In particular, it incorporates ten PRISMA elements with an emphasis on transparency in data sourcing, clear articulation of the search strategy, definition of the time horizon, and a high-level description of the screening process. At the same time, it intentionally excludes elements such as protocol preregistration, exhaustive database coverage, formal risk-of-bias assessment, and detailed audit trails of inclusion and exclusion decisions. The primary objective is conceptual synthesis and framework development rather than statistical aggregation or comprehensive evidence consolidation. Narrative reviews are especially suitable for integrating heterogeneous bodies of the literature, proposing new classifications, interpreting emerging thematic structures, and developing conceptual models, which represent the main contributions of this study. The analyzed literature spans multiple domains, including artificial intelligence, industrial automation, cybersecurity, and Industry 5.0, and is characterized by variability in reporting standards and experimental contexts, particularly regarding energy-related metrics, which limits the feasibility and reliability of a fully systematic synthesis. The partial adoption of PRISMA 2020 principles strengthens methodological transparency by documenting the search period, keyword selection, eligibility logic, and inclusion process, while explicitly acknowledging that the dataset is not exhaustive or statistically representative. Accordingly, quantitative outputs such as cluster distributions and percentage values are presented in a descriptive and exploratory manner, consistent with the objectives of a narrative review and supporting an integrated, interpretive, and forward-looking analysis while maintaining appropriate methodological clarity and reader expectations.

3.2. General Results of Analysis

Figures 5 and 6 and Tables 2–7 present a summary of the bibliometric analysis results. The final dataset comprises 82 articles published within the last decade, covering the period from January 2016 to June 2026. Earlier publications were excluded due to the

rapid evolution of the research field, which has significantly reduced the relevance of older studies.

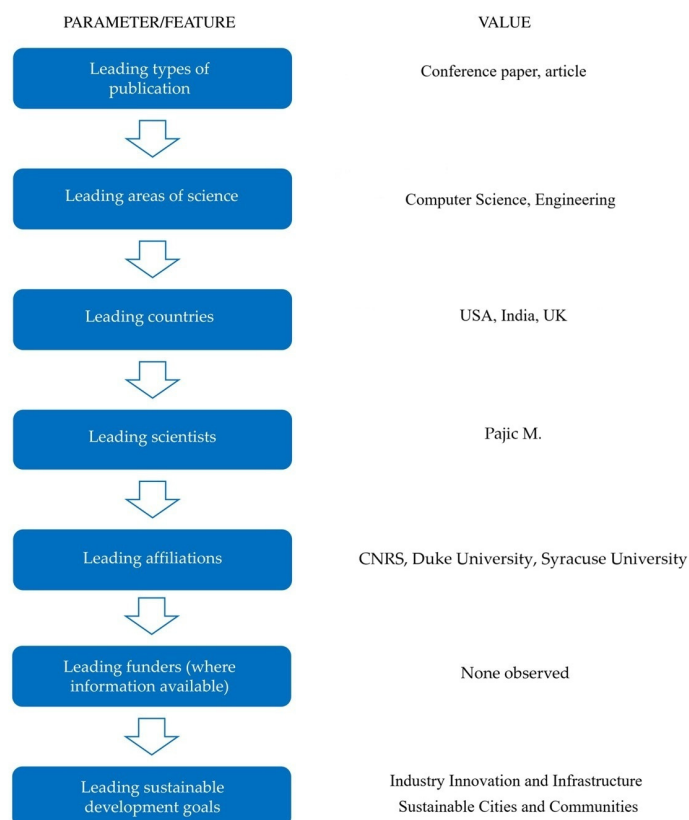


Figure 5. Bibliometric analysis results aggregated from all selected databases, including Web of Science (WoS), Scopus, PubMed, and DBLP.

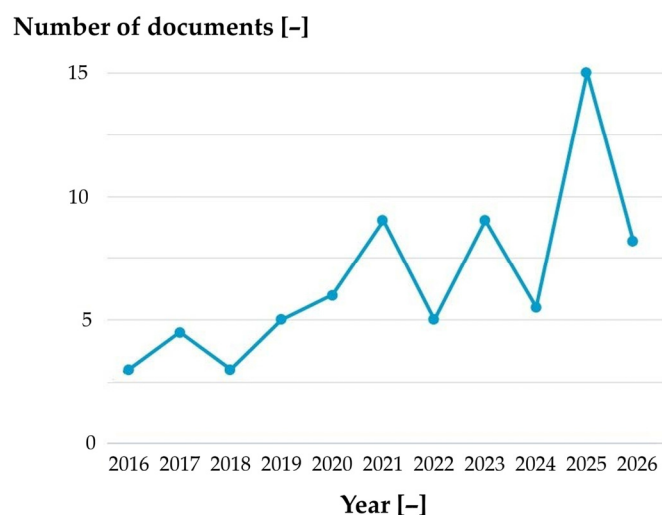


Figure 6. Documents by year.

The bibliometric results suggest that the high proportion of journal articles and conference papers reflects a research domain that is still largely in an exploratory and conceptual phase, with a stronger emphasis on proposed architectures than on large-scale practical implementations. The significant representation of computer science, engineering, and mathematics further indicates that the field is still in its early stages of technological maturation. While countries such as India, the United States, and China demonstrate the highest levels of research activity, no single author or institution shows clear dominance, pointing

to a fragmented and highly distributed research landscape. In addition, the most frequently addressed Sustainable Development Goals highlight a focus on industrial applications and development-oriented objectives.

Table 2. Documents by type.

Document Type	Percentage [%]
Conference paper	49.0
Article	25.5
Review	6.9
Book chapter	9.7
Book	4.1
Conference review	4.1
Editorial	0.7

Table 3. Documents by subject area.

Subject Area	Percentage [%]
Computer Science	34.9
Engineering	25.9
Mathematics	9.0
Energy	4.7
Decision Sciences	4.4
Social Sciences	4.4
Physics and Astronomy	3.1
Business, Management, and Accounting	2.5
Material Science	2.5
Environmental Science	2.2
Others	6.4

Table 4. Documents by country/territory (top 5).

Country	Number of Documents [-]
USA	20
India	12
UK	6
China	4
Australia	3

Table 5. Documents by affiliation.

Affiliation	Number of Documents [-]
CNRS	3
Duke University	2
Syracuse University	2

Table 6. Documents by author.

Author	Number of Documents [-]
Pajic M.	3

Table 7. Documents by SDGs.

SDG	Number of Documents [-]
Industry Innovation and Infrastructure	8
Sustainable Cities and Communities	7
Responsible Consumption and Production	5
Good Health and Wellbeing	4
No Poverty	2

Not all studies included in the review explicitly referenced the SDGs, and SDG alignment was not used as a criterion during the publication selection process. Although the United Nations has established the SDGs as a global framework for 2030, their adoption is not uniformly required across all countries, institutions, or research communities. By incorporating both studies that explicitly mention the SDGs and those that do not, the review captures a broader spectrum of perspectives, enabling an assessment of how sustainability considerations are addressed in the literature and the extent to which they are explicitly or implicitly reflected in research practices across different institutional and national contexts.

As Cyber-Physical Systems 2.0 (CPS 2.0) become more complex and autonomous, they are increasingly exposed to sophisticated security threats and privacy risks. The integration of AI-driven decision-making introduces additional attack vectors that can potentially be exploited to manipulate system behavior. In large-scale IoT ecosystems comprising thousands or even billions of interconnected devices, the attack surface expands significantly, making intrusion detection, monitoring, and system resilience more challenging. At the same time, privacy concerns intensify, as CPS 2.0 processes sensitive data related to individuals, industrial operations, and critical infrastructure. Building trust in such environments requires not only robust cryptographic mechanisms but also comprehensive security frameworks aligned with regulatory and compliance standards [16]. Future CPS 2.0 architectures must therefore adopt a security-by-design approach, incorporating threat modeling, anomaly detection, and real-time autonomous defense mechanisms [2,17]. Ultimately, effectively addressing these challenges is crucial for maintaining public trust and enabling the secure deployment of CPS 2.0 across domains such as energy systems, healthcare, transportation, and smart city infrastructures.

3.3. Technical Issues

CPS 2.0 encounters significant technical challenges, as conventional centralized security architectures often introduce latency that limits real-time threat detection and response capabilities. Scalability is also a critical issue, since centralized infrastructures struggle to process the vast and continuous data streams generated by Industry 4.0 and Industry 5.0 environments. In addition, concerns regarding data sensitivity restrict the practicality of transmitting raw data to centralized servers for analysis [18]. To address these limitations, AI and ML, including GenAI, are increasingly being adopted to enable more adaptive and autonomous threat detection mechanisms. However, deploying AI models within CPS 2.0 requires careful resource optimization, as edge devices typically operate under constrained computational and energy capacities. Edge computing helps mitigate latency and reduce data exposure risks, but it also introduces challenges in coordinating

distributed intelligence across heterogeneous and geographically dispersed nodes. FL provides a privacy-preserving alternative for collaborative model training; nevertheless, it faces limitations such as communication overhead, model drift, and variability in data quality across participating devices. The integration of GenAI with FL-based architectures further raises security concerns, particularly related to adversarial attacks, model poisoning, and manipulation of training processes. Ensuring seamless interoperability among GenAI, FL, and edge computing therefore requires robust orchestration mechanisms and standardized communication protocols [19]. CPS 2.0 must overcome these challenges to achieve a scalable, adaptive, and proactive cybersecurity framework capable of countering increasingly sophisticated threats in highly interconnected environments.

CPS 2.0 infrastructure integrates physical processes, cyber components, and intelligent services into a unified ecosystem designed for resilience, adaptability, and scalability. At its foundation, edge computing nodes perform local data processing near the source of generation, thereby reducing latency and minimizing dependence on centralized infrastructures. Cloud platforms complement this architecture by offering large-scale storage, advanced analytics, and orchestration of distributed resources. AI and ML models, including GenAI, constitute the cognitive layer, enabling predictive maintenance, anomaly detection, and autonomous decision-making capabilities [20]. FL frameworks interconnect distributed nodes, allowing collaborative model training without the exchange of raw data, thus enhancing privacy and data protection. A secure and high-performance communication backbone, supported by technologies such as 5G, IoT, and software-defined networks (SDN), ensures reliable, low-latency connectivity across heterogeneous devices and domains. Embedded cybersecurity mechanisms span the entire infrastructure, incorporating encryption, authentication, intrusion detection, and adaptive threat response techniques. Digital twin technologies further enhance system intelligence by simulating physical environments for performance optimization and enabling the testing of security strategies in virtual settings prior to real-world deployment. Interoperability across diverse industrial systems is achieved through standardized Application Programming Interfaces (APIs), middleware solutions, and communication protocols that support seamless integration [21]. CPS 2.0 infrastructure is decentralized, intelligent, and adaptive, specifically designed to satisfy the evolving requirements of Industry 4.0 and Industry 5.0 while ensuring scalability, reliability, and trustworthiness (Figure 7).

Paper [22] introduces a blockchain-enabled authentication framework for cyber-physical transportation systems operating in a cloud-edge environment, offering privacy protection, unconditional anonymity, and efficient batch verification of data while reducing the complexity of key management. The proposed approach employs elliptic curve cryptography to construct a pairless ring signature scheme, which significantly decreases computational and resource overhead. Authentication is executed directly on the blockchain, thereby enhancing the trustworthiness and reliability of vehicle-to-vehicle and vehicle-to-infrastructure communications. The security of the scheme is formally validated under the elliptic curve discrete logarithm assumption within the random oracle model, while experimental evaluations demonstrate that it is both practical and more efficient than existing methods [22]. The increasing adoption of edge computing and IoT technologies in Industry 4.0 has intensified the sophistication of advanced persistent threats, revealing the limitations of traditional security mechanisms in safeguarding cyber-physical systems within zero-trust environments. In response, a subsequent study proposes a federated learning and blockchain-integrated intrusion detection system (FL-BIDPS) that enables decentralized, privacy-preserving threat detection along with tamper-resistant logging of security events. By eliminating the need to share raw data and enabling collaborative model training, this approach enhances scalability, system performance, and resilience against

advanced persistent threats compared to conventional techniques [23]. Mobile edge computing improves service quality by offloading computational tasks to high-performance edge servers; however, it also introduces significant challenges related to security and data privacy. To mitigate these risks, another study integrates federated learning within cyber–physical systems, enabling improved data utility while preserving privacy, and further examines the dynamic and unpredictable nature of cyberattacks, particularly in environments supported by unmanned aerial vehicles. Rather than relying on predefined attack signatures, the study analyzes system behavior under attack conditions, highlighting that while simple and repetitive attacks can be detected efficiently, more sophisticated adversaries may evade detection through adaptive and carefully engineered strategies [24]. CPS 2.0 are extensively deployed in domains such as healthcare, agriculture, and transportation to automate processes and minimize human intervention. However, conventional ML approaches raise significant concerns related to data leakage and privacy risks. FL partially mitigates these issues by enabling local model training and sharing only model updates, thereby improving privacy protection, although residual risks of information leakage may still persist. To further strengthen data privacy, one study introduces a differential privacy mechanism that injects controlled noise into the data, ensuring anonymity while simultaneously evaluating its effects on model accuracy and data quality [25]. A related study provides a systematic review of cybersecurity challenges and solutions in cyber–physical systems within industrial IoT (IIoT) edge computing environments. It identifies prevalent attack vectors, intrusion methods, and key security threats, while also proposing a taxonomy of existing security mechanisms and comparing them with current state-of-the-art approaches. The analysis highlights common system vulnerabilities and underscores the importance of integrating advanced technologies such as machine learning, federated learning, blockchain, and cryptographic techniques. It further outlines future research directions aimed at strengthening CPS 2.0 security in complex IIoT environments [26]. CPS 2.0 integrates computational intelligence with physical processes to enable real-time monitoring, decision-making, and automation; however, deploying GenAI in such distributed and data-sensitive environments introduces significant privacy and security challenges. To address these issues, a proposed Generative Proxy Learning Framework combines proxy-based federated learning with diffusion models to generate high-quality synthetic data while enabling secure collaboration through both private and shared model components. The framework enhances privacy using differential privacy and encryption techniques, and experimental results demonstrate improved performance, reduced data leakage, and higher accuracy in anomaly detection and predictive tasks within CPS 2.0 environments [27]. The integration of CPS 2.0 with edge computing has also enhanced the efficiency of intelligent logistics systems, particularly those involving multiple autonomous guided vehicles. One study addresses complex planning and scheduling challenges by introducing a time-constrained virtual network mapping approach combined with an improved A* algorithm adapted to logistics scenarios. In addition, a proactive traffic control mechanism is proposed to improve scheduling efficiency and collision avoidance, with experimental results showing significant gains in system performance, safety, and operational efficiency [28]. The rapid expansion of IoT-based applications has resulted in the continuous generation of large volumes of sensitive data, while advancements in networking technologies such as SDN and edge computing have significantly improved system flexibility and performance. In the context of evolving CPS and IoT, challenges related to latency management and secure computation offloading remain critical, even with the integration of cloud and edge computing paradigms. To address these issues, one study proposes a deep learning-based federated efficient offloading scheme alongside a privacy-preserving federated learning framework tailored for CPS environments [29].

CPSs also play a central role in enabling intelligent and secure control within emerging 5G and 6G network infrastructures. However, the rapid proliferation of smart devices in urban environments introduces resource constraints, limiting the ability of local systems to process intensive workloads. Although mobile edge computing helps alleviate this burden by offloading computational tasks, traditional terrestrial infrastructure often fails to meet ultra-low latency requirements, which has led to the deployment of additional MEC servers to support dynamic and emergency scenarios. To address complex optimization and decision-making challenges in such environments, a hierarchical deep federated learning framework has been proposed, demonstrating improved energy efficiency, enhanced resource allocation, and better performance, privacy, and quality of service in simulation studies [30]. Artificial intelligence is also expected to be a key enabler of 6G-supported edge computing in eHealth applications, where cyber-physical systems integrate wearable devices and smartphones. However, these systems remain vulnerable to sophisticated threats such as blackhole and greyhole attacks, which are difficult to detect with traditional methods. To mitigate these risks, another study introduces an optimized smart healthcare framework that integrates advanced machine learning techniques with a federated decentralized authentication model to enhance both data security and analytical accuracy. Experimental evaluations confirm strong performance across multiple metrics, demonstrating significant improvements in healthcare data protection within CPS environments [31]. FL enables multiple clients to collaboratively train a shared global model while preserving data locality, and its extension—federated continuous learning—supports adaptation to evolving tasks and dynamic data distributions. To address challenges related to client-level personalization and catastrophic forgetting in heterogeneous data settings, a subsequent study proposes the Meta-RBCIL algorithm, which meta-trains a representation network under a federated learning paradigm and adapts it to individual clients using balanced gradient updates. Experimental results indicate that Meta-RBCIL outperforms baseline methods in terms of task accuracy, reduces forgetting, and improves generalization, making it well-suited for deployment in edge computing environments [32]. Smart grids, as safety-critical cyber-physical systems, are highly exposed to cyber threats, with false data injection attacks (FDIA) representing one of the most severe security challenges. To address this issue, a privacy-preserving FDIA detection framework is proposed that combines Transformer-based models, FL, and the Paillier cryptosystem, enabling edge nodes to collaboratively analyze electrical measurements while maintaining the confidentiality of local data. Experimental evaluations conducted on IEEE 14-bus and 118-bus systems demonstrate that the proposed method effectively detects FDIAs while preserving data privacy and outperforming existing approaches [33]. Although many recent studies have introduced task-specific models and algorithms, relatively few have addressed the integration of CPSs into broader computational paradigms, leaving a gap in unified frameworks. To bridge this gap, one study investigates CPS integration with cloud, fog, and edge computing environments, analyzing their applications, algorithmic approaches, and optimization strategies for big data processing, while also identifying existing limitations and outlining future research directions [34]. Smart homes, as essential components of smart cities and representative human-cyber-physical systems (HCPS), increasingly rely on artificial intelligence to deliver intelligent services. However, sending data to centralized cloud platforms for model training introduces significant privacy risks. To mitigate this, a hybrid edge computing approach is proposed that enables local training of deep learning models while keeping sensitive data within trusted environments, while still coordinating with cloud systems through federated learning. Experimental results confirm that this approach is both feasible and effective for secure and efficient AI deployment in smart home ecosystems [35]. The next article presents a cloud-based diagnostic framework for the remote assessment of

security issues in critical infrastructure using CPSs. The approach adapts two architectural design patterns:

- Ambassador pattern to extend CPS input interfaces to cloud services.
- Data Aggregation pattern to extend output interfaces.

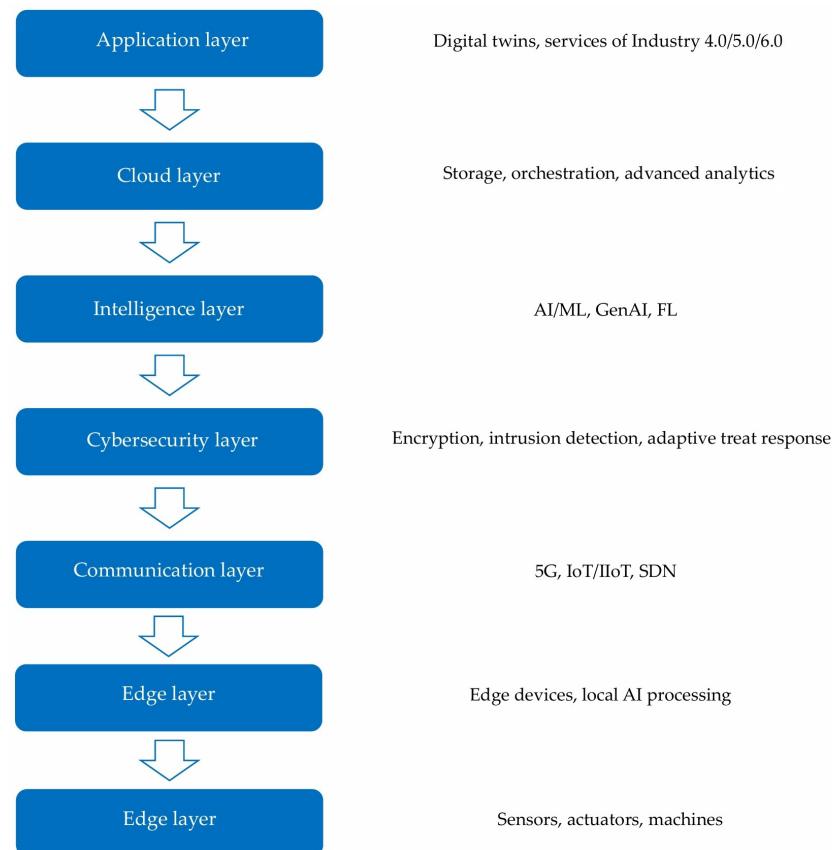


Figure 7. Layered representation of the CPS 2.0 infrastructure illustrating how the system is organized from physical devices at the base layer to application-level services at the top.

Thereby addressing challenges associated with remote security monitoring. Implementation and evaluation in a simulated environment demonstrate that the proposed method improves both the accuracy and efficiency of security diagnostics, supporting the development of more secure and reliable CPS 2.0 infrastructures [36]. The healthcare sector has experienced a growing number of cybersecurity threats driven by the increasing integration of diverse digital technologies within smart healthcare environments, where traditional security mechanisms are often inadequate. To address these challenges, a Privacy-Enhanced Federated Cyber Physical and Attack Detection (PEF-CAPD) framework is proposed, combining edge computing, cloud computing, and federated learning (FL) to preserve data privacy while enabling effective attack detection. In this approach, patient-specific local models are trained at the edge and subsequently aggregated into a global model to enhance threat detection capabilities. Experimental validation on benchmark healthcare datasets shows that PEF-CAPD achieves an accuracy of 99.92%, outperforming existing state-of-the-art methods [37]. Integrating ML with CPSs remains challenging due to stringent requirements for real-time decision-making, security, reliability, device heterogeneity, and data privacy. Federated learning, as a decentralized ML paradigm, has gained significant attention in CPSs by enabling model training on distributed data sources while jointly integrating computational, communication, and physical processes. This study provides a comprehensive overview of federated learning-enabled CPSs (FL-CPS), covering applica-

tions, system architectures, algorithmic designs, and key findings, while also comparing CPS and IoT use cases and identifying open challenges and future research directions [38]. Cyber-physical systems are inherently vulnerable to attacks due to their tight integration of cyber and physical components. To enhance security, end-to-end homomorphic encryption (HE) has been proposed to enable computations over encrypted data. However, existing HE-based comparison methods are computationally expensive because they require multiple iterative operations, limiting their practicality in real-world CPS deployments. To overcome this limitation, a novel method based on asymmetric input scaling and parallel multi-level thresholding is introduced, achieving comparable accuracy while reducing execution time by 48% on edge devices, with further improvements of up to 63% when additional parallel processing threads are applied [39]. Cyber-physical systems combine computational intelligence with physical processes, and edge computing has become a key enabler for addressing constraints related to latency, energy consumption, accuracy, and bandwidth in cloud-centric architectures. This study analyzes critical performance metrics in edge-assisted CPS (EaCPS), including latency, energy efficiency, accuracy, scalability, security, and reliability. It also reviews traditional CPS models and their evolution under edge computing paradigms, evaluates AI-integrated CPS architectures, identifies emerging research trends and challenges, and proposes strategies for optimizing the performance of EaCPS systems [40]. Underwater drones are widely used in scientific exploration, environmental monitoring, and maritime operations; however, their effectiveness is limited by low bandwidth, high latency, signal attenuation, and intermittent connectivity, which make centralized data processing inefficient and unreliable. To overcome these constraints, one study proposes an FL framework that enables underwater drones to collaboratively train a global intrusion detection model locally while sharing only model updates instead of raw data. This approach strengthens cybersecurity in underwater networks by preserving sensitive information, supporting decentralized anomaly detection, and improving the detection of threats, including zero-day attacks, within the Internet of Underwater Things (IoUT) [41]. Another study introduces a Zero-Trust security framework for 6G-enabled CPSs, integrating adaptive access control, end-to-end encryption, and blockchain technology to enhance scalability, security, and real-time threat detection. By removing implicit trust assumptions and incorporating AI-driven anomaly detection alongside blockchain-based authentication, the framework mitigates threats such as man-in-the-middle (MITM) attacks, distributed denial-of-service (DDoS) attacks, and data breaches, while ensuring tamper-resistant data integrity and decentralized access management. Experimental results indicate substantial improvements in latency, authentication performance, and overall attack resilience, demonstrating its suitability for securing large-scale, mission-critical CPS 2.0 applications in domains such as healthcare, smart infrastructure, and industrial automation [42]. Network traffic classification and anomaly detection are essential for ensuring secure and efficient network operations; however, existing FL approaches struggle with non-stationary data distributions and class-incremental learning scenarios. To address these limitations, a study proposes MCFL, a class-incremental FL framework that integrates dynamic network representation learning with a multi-scale expert-based feature fusion mechanism to capture evolving traffic patterns across both temporal and spatial dimensions. By incorporating an incremental distribution loss function, MCFL effectively reduces catastrophic forgetting and class imbalance issues, achieving an average performance improvement of 6.04% over baseline methods across multiple network traffic datasets [43]. The rapid proliferation of connected devices has driven the development of complex cyber-physical systems, where Edge Intelligence Systems (EIS) combine edge computing and artificial intelligence to deliver low-latency, intelligent services for applications such as Intelligent Transportation Systems (ITS). However, conventional EIS architectures that rely on centralized aggregation

servers face significant security vulnerabilities and challenges in system orchestration. To address these issues, a secure Edge Intelligence framework is proposed that integrates federated learning, blockchain technology, and Local Differential Privacy (LDP) to enhance traffic forecasting accuracy, decentralize system management, and protect user privacy through immutable data records and randomized privacy-preserving mechanisms [44]. Mobile Cyber-Physical Systems (MCPS) extend the functionality of traditional CPSs, enabling applications in areas such as intelligent transportation, smart homes, and mobile learning environments. However, these systems face significant challenges, including large-scale data transmission, high communication overhead, and data security risks. To address these issues, one study proposes NESPS, a secure and efficient edge computing-based data sharing and privacy-preserving framework that reduces communication costs and optimizes interactions between devices and cloud environments. By incorporating attribute-based encryption for fine-grained access control and validating its performance through security analysis and simulations, NESPS demonstrates strong effectiveness in preserving data privacy while ensuring efficient operation of MCPSs [45]. The increasing integration of smart grids and computational technologies in industrial environments has intensified cyber threats targeting cyber-physical systems, exposing the limitations of traditional intrusion detection systems that depend on large, high-quality datasets. To overcome these challenges, the federated EEFED (Execution & Evaluation Dual Network Framework) is introduced, enabling participants to train personalized local models while collaboratively constructing a robust global detection model. Through a personalized update mechanism and optimized backtracking parameter strategy, EEFED enhances model stability and robustness. Experimental evaluations on network datasets show that it outperforms both single-model baselines and state-of-the-art approaches, particularly in handling imbalanced and non-identically distributed data [46]. The growth of Industry 4.0 has driven widespread adoption of industrial cyber-physical systems (ICPSs), which tightly integrate physical processes with computational intelligence but remain highly vulnerable to cyber threats, highlighting the need for effective intrusion detection systems (IDSs). To address challenges related to privacy, scalability, and computational complexity, a lightweight federated deep learning-based IDS called FedSecureIDS is proposed. It combines convolutional neural networks (CNNs), long short-term memory (LSTM) networks, and multilayer perceptrons (MLPs) within a federated learning framework, while ensuring secure communication through symmetric session key exchange and mutual authentication. Experimental results demonstrate that FedSecureIDS achieves high accuracy, precision, recall, and F1-score on edge devices, with performance comparable to centralized IDS solutions, while formal security analysis confirms strong resilience against known attacks and robust privacy protection [47]. Edge computing enhances data-driven analytics by bringing computation closer to data sources, thereby reducing bandwidth usage and improving security. However, the limited resources of edge devices make them susceptible to software aging, which can degrade system performance over time. To address this issue, a study proposes a deterministic and stochastic Petri net (DSPN) model to quantitatively evaluate the effects of software aging in cyber-physical systems, using anomaly detection in a wastewater treatment plant as a case study. Simulation and numerical results indicate that software aging negatively affects key performance indicators, including detection loss probability and false positive rates, underscoring the importance of accounting for aging effects in edge-enabled CPS environments [48]. Side-channel attacks, including those exploiting magnetic field leakage or differential power analysis, represent a significant threat to CPS 2.0, as they target unmonitored communication channels and open-loop system behaviors. To address this issue, a novel out-of-band data exfiltration approach is proposed, which exploits previously unobserved physical system dynamics and demon-

strates that reliance on state estimation-based intrusion detection alone is insufficient to fully mitigate stealthy data theft. The method is evaluated using two real-world testbeds—a robotic arm control system and an autonomous surveillance drone—and is accompanied by an analysis of potential defense mechanisms and their inherent limitations [49]. The rapid advancement of deep learning and edge computing presents new opportunities for modernizing university administrative systems, which often struggle to adapt to highly dynamic and complex operational environments. In this context, a CPS-integrated video signal processing framework based on deep convolutional neural networks is developed to enable scalable, real-time network management, monitoring, and enhanced campus security. The proposed modular architecture supports the deployment of cloud agents on edge devices, improving video processing efficiency, operational performance, and system stability, while also providing a scalable foundation for future technological expansion [50]. Vehicular Cyber-Physical Systems (VCPSs) are a fundamental component of intelligent transportation systems and smart city development, attracting extensive research from academia, industry, and government, and leveraging technologies such as SDN, blockchain, cloud computing, and machine learning. Recently, mobile edge computing (MEC) has been adopted to optimize content caching and resource allocation, enabling low-latency, data-intensive vehicular applications that enhance the driving experience. To address growing concerns related to security and privacy, a federated learning framework combined with differential privacy is proposed, allowing distributed model training at the edge while preserving local vehicular data and improving resilience against adversarial attacks [51]. A vision of a sustainable and intelligent future envisions people, infrastructure, and natural systems integrated within a unified cyber-physical ecosystem, where the reliability and sustainability of energy systems become critical. Battery-backed energy storage systems play a key role in stabilizing power supply and enabling load balancing. However, early fault detection remains challenging due to limited anomaly data and privacy constraints. To address this, a federated anomaly detection approach is proposed that trains global autoencoder models using only normal operational data without sharing sensitive information. Experimental results demonstrate that the method enables accurate and timely detection of battery anomalies immediately after deployment while preserving data privacy [52]. EIS, which integrate artificial intelligence with edge computing, are increasingly deployed to deliver low-latency and high-performance intelligent cloud services, particularly in Intelligent Transportation Systems (ITS) within vehicular networks. However, conventional EIS architectures that rely on centralized aggregation mechanisms remain vulnerable to various security threats. To address these limitations, this study proposes a decentralized edge intelligence framework that integrates FL, differential privacy (DP), and blockchain technology to enable secure data management, tamper-resistant transaction recording, and enhanced traffic prediction. The framework implements FL with differential privacy to safeguard user data and combines FL with blockchain to ensure secure and transparent traffic management processes. Simulation results demonstrate that the proposed approach achieves high privacy guarantees while maintaining strong predictive performance, with accuracy levels of 95.8%, 93.78%, and 89.31%, respectively, indicating substantial improvements in both privacy preservation and system performance in vehicular network environments [53,54].

These technologies complement, not compete. AI/ML provides an analytical foundation, enabling intelligent threat detection and predictive cybersecurity. However, centralized AI approaches face limitations in scalability, latency, and privacy in large-scale CPS and IoT environments. Edge computing addresses these challenges by bringing computation closer to the data source, enabling low-latency detection and response while reducing communication overhead. FL further enhances distributed intelligence by enabling collaborative model training without exposing sensitive local data, although it introduces

challenges related to model heterogeneity, communication efficiency, and poisoning attacks. GenAI extends the capabilities of conventional AI by supporting automated threat analysis, incident response, security policy generation, and cyber defense decision support. Despite its significant potential, its implementation in critical CPS environments is still limited by concerns about reliability, explainability, hallucinations, and secure implementation. DTs provide complementary capabilities by creating virtual replicas of physical assets, enabling predictive monitoring, cyberattack simulation, and resilience assessment without disrupting operational systems. The literature points to a shift from isolated AI techniques to integrated security architectures combining AI/ML, FL, edge computing, GenAI, and DTs. Such integrated frameworks offer significant potential for achieving autonomy, adaptability, and privacy-preserving cybersecurity in CPS 2.0. However, they also raise new research challenges related to interoperability, trust management, explainability, standardization, secure orchestration, and validation in real-world industrial environments. These challenges constitute key directions for future research on resilient Industry 5.0 ecosystems (Table 8).

Table 8. Comparative summarization AI/ML, federated learning, edge computing, GenAI, and DTs approaches.

Technology/ Approach	Primary Role in CPS 2.0 Security	Strengths	Limitations/ Challenges	Typical Applications	Research Maturity
AI/ML	Intelligent threat detection, anomaly detection, malware classification, predictive analytics	High detection accuracy; capability to identify unknown threats; adaptive learning; supports automation of security operations	Requires large, high-quality datasets; vulnerable to adversarial attacks and data poisoning; limited explainability; computationally intensive for deep models	Intrusion Detection Systems (IDS), malware detection, network traffic analysis, industrial anomaly detection, predictive maintenance	High—extensively studied with numerous experimental and industrial implementations
FL	Privacy-preserving collaborative model training across distributed CPS/IoT nodes	Preserves data privacy; reduces raw data transmission; supports distributed intelligence; improves regulatory compliance	Non-IID data reduces model performance; communication overhead; model poisoning attacks; client heterogeneity; synchronization complexity	Distributed IDS, collaborative threat intelligence, smart factories, healthcare IoT, smart grids	Medium-to-High—rapidly growing research field with limited large-scale industrial deployment
Edge computing	Local processing and real-time security analysis close to data source	Low latency; reduced bandwidth consumption; improved privacy; faster incident response; supports autonomous operation	Limited computing and energy resources; distributed management complexity; edge node security; scalability issues	Industrial IoT, autonomous vehicles, smart manufacturing, robotics, smart cities	High—widely adopted in Industry 4.0 with increasing integration into cybersecurity architecture

Table 8. Cont.

Technology/ Approach	Primary Role in CPS 2.0 Security	Strengths	Limitations/ Challenges	Typical Applications	Research Maturity
GenAI	Automated threat analysis, attack simulation, incident response assistance, security policy generation, cyber defense decision support	Generates contextual security insights; supports automated response; accelerates security analysis; enhances SOC operations; enables adaptive defense strategies	Hallucinations; reliability concerns; prompt injection attacks; model misuse; high computational cost; explainability and governance challenges	Security assistants, vulnerability analysis, attack scenario generation, SOC automation, cyber training, threat intelligence	Medium—rapidly emerging field with growing research activity but limited operational validation in critical CPS environments
DTs	Virtual representation of physical CPSs for monitoring, simulation, risk assessment, and resilience evaluation	Enables predictive analysis; safe testing environment; continuous monitoring; supports proactive defense; improves system resilience	High implementation complexity; synchronization accuracy; interoperability challenges; computational overhead; cybersecurity of the twin itself	Industrial control systems, smart manufacturing, predictive maintenance, infrastructure monitoring, cyberattack simulation	Medium—increasing industrial adoption, but cybersecurity-focused implementations remain relatively limited
Integrated AI + FL + Edge + GenAI + DT Framework	Autonomous, adaptive, distributed cybersecurity ecosystem	Combines real-time intelligence, privacy preservation, predictive capabilities, resilience, and autonomous decision-making; suitable for CPS 2.0	Architectural complexity; interoperability; orchestration of heterogeneous components; trust management; standardization; lifecycle management	Industry 5.0, autonomous factories, critical infrastructure, smart energy systems, resilient IoT ecosystems	Emerging—recognized as a promising research direction with relatively few comprehensive real-world deployments

3.4. Cross-Cutting Trade-Offs in AI-Based Autonomous Security for CPS 2.0

While AI, FL, edge computing, GenAI, and DTs significantly enhance the security of CPS 2.0 systems, their implementation inevitably involves balancing conflicting design goals. No single technology simultaneously optimizes security, privacy, latency, scalability, computational efficiency, and operational costs. In reality, autonomous cybersecurity architectures must carefully consider several trade-offs.

3.4.1. Security vs. Latency

Fast threat detection and response are essential for critical CPS applications such as industrial automation, autonomous transportation, and smart energy systems. Cloud-centric security architectures typically provide access to powerful computing resources capable of executing advanced AI models. However, transmitting sensor data to remote cloud platforms introduces communication delays that can prevent a rapid response to

cyberattacks. Edge computing addresses this limitation by moving AI inference closer to the data source, enabling near-real-time intrusion detection and autonomous decision-making. Although edge computing significantly reduces latency, edge devices typically have limited processing power, memory, and energy resources, limiting the complexity of deployable AI models. Therefore, system designers must balance inference accuracy with computational efficiency when implementing security mechanisms at the edge.

3.4.2. Privacy and Detection Accuracy

AI-based cybersecurity solutions generally improve as larger and more diverse datasets become available for model training. However, aggregating sensitive operational data from distributed CPS components can expose confidential industrial processes, proprietary information, or personal data. Federated learning mitigates these concerns by allowing multiple devices to jointly train shared models without exchanging raw data. While this significantly enhances privacy protection and regulatory compliance, federated learning often suffers from reduced model accuracy due to non-independent and non-identically distributed datasets, heterogeneous client capabilities, and intermittent communication. Furthermore, cooperative learning remains vulnerable to model poisoning and inference attacks, requiring additional security mechanisms such as secure aggregation, differential privacy, and robust aggregation algorithms.

3.4.3. Centralized vs. Distributed Security Architectures

Traditional cybersecurity architectures rely on centralized monitoring and decision-making, offering unified visibility, simplified policy management, and a relatively simple maintenance model. However, centralized systems can become performance bottlenecks and present attractive single points of failure, especially in large-scale IoT ecosystems encompassing thousands of heterogeneous devices. Distributed security architectures based on edge computing and federated intelligence improve scalability, resilience, and fault tolerance by enabling local decision-making and reducing dependence on central infrastructure. However, decentralization increases architectural complexity, requiring distributed coordination, synchronization, trust establishment, and consistent enforcement of security policies across multiple autonomous nodes. It must be acknowledged, however, that hybrid architectures combining centralized supervision with decentralized intelligence have emerged as a promising compromise for CPS 2.0 environments.

3.4.4. Intelligence vs. Explainability

DL and GenAI have demonstrated remarkable capabilities in detecting advanced cyber threats, predicting attack patterns, and automating incident response. However, many of these models operate as “black boxes,” providing limited insight into the rationale behind their decisions. For safety-critical CPS applications, explainability is essential for building operator trust, facilitating forensic investigations, and meeting regulatory requirements. XAI techniques improve model transparency but often incur additional computational overhead and can simplify decision boundaries, potentially reducing predictive performance. Striking a balance between prediction accuracy and interpretability therefore remains a key research challenge.

3.4.5. Adaptability vs. Resilience

Modern cyber threats are constantly evolving, requiring AI models that can adapt to new attack vectors and changing operating environments. Online learning, reinforcement learning, and GenAI provide adaptive capabilities that enable continuous model improvement. However, increased adaptability can also lead to instability, catastrophic forgetting, or vulnerability to adversarial manipulation. Autonomous learning systems must there-

fore carefully regulate model updates while ensuring resilience to adversarial examples, data poisoning, and concept drift. Maintaining this balance is particularly important in industrial CPSs, where erroneous autonomous decisions can have serious security and economic consequences.

3.4.6. Model Complexity and Resources Efficiency

Large-scale deep neural networks and fundamental models typically achieve better predictive performance but require significant computational, memory, and energy resources. Such requirements are often incompatible with resource-constrained IoT devices deployed in CPS environments. Model compression, pruning, knowledge distillation, lightweight neural architectures, and hardware-aware optimization techniques have emerged as practical solutions for implementing AI on edge devices. However, reducing model complexity can reduce detection accuracy and generalization capabilities, illustrating the inherent tradeoff between computational efficiency and cybersecurity performance.

3.4.7. Automation vs. Human Oversight

The increasing integration of AI enables the creation of highly autonomous cybersecurity systems capable of detecting threats, generating alerts, and initiating remediation with minimal human intervention. This autonomy significantly improves response speed and reduces operational burden. Despite these advantages, fully autonomous decision-making can lead to erroneous responses, false alarms, or unintended disruptions to physical processes. Experts remain essential for validating critical security decisions, interpreting complex attack scenarios, and managing exceptional situations. Therefore, current research increasingly favors “human-in-the-loop” and “human-on-the-loop” architectures that combine AI-based automation with expert oversight.

3.4.8. Implications for Future CPS 2.0 Security Architectures

The reviewed literature demonstrates that future CPS 2.0 security solutions will not rely on a single technology but will integrate AI/ML, edge computing, federated learning, GenAI, and DTs within collaborative security ecosystems. The effectiveness of these architectures depends on achieving appropriate trade-offs between latency, privacy, scalability, explainability, computational efficiency, and operational resilience. Therefore, future research should focus on developing adaptive architectures capable of dynamically balancing these conflicting goals, depending on application requirements, resource availability, and evolving cyberthreats. Such adaptive optimization will be essential to realizing secure, resilient, and trustworthy autonomous CPS infrastructures in Industry 5.0 and beyond.

3.5. Observed Technological Research Gaps and Challenges

A review of the scientific literature indicates significant progress in applying AI to secure CPS 2.0 and IoT ecosystems. AI, ML, FL, edge computing, GenAI, and DTs collectively constitute the foundation for autonomous cybersecurity, capable of detecting, predicting, and responding to increasingly sophisticated cyberthreats. However, the current state of research remains fragmented, with many proposed solutions addressing specific aspects of the security problem, while only a small portion of work considers comprehensive, end-to-end, autonomous security architectures. Several cross-cutting research gaps emerge in the scientific literature.

3.5.1. Lack of Integrated Security Architectures

Most existing studies analyze intrusion detection based on AI, FL, edge intelligence, DTs, or GenAI as standalone technologies. While each approach demonstrates distinct advantages, relatively few studies propose unified architectures that combine these comple-

mentary capabilities into a coherent security framework. Future research should therefore focus on developing an integrated CPS security architecture capable of coordinating distributed intelligence, predictive analytics, privacy protection, and autonomous response in heterogeneous IoT environments.

3.5.2. Limited Validation in Real-World CPS Environments

A significant portion of published research evaluates proposed methods using simulations, test datasets, or laboratory testbeds. While these studies provide valuable proof-of-concept, they often fail to address the complexity, heterogeneity, and operational constraints of industrial CPS implementations. Large-scale experimental validation in smart factories, industrial control systems, smart energy grids, healthcare infrastructure, and autonomous transportation remains relatively rare. Future work should emphasize realistic deployment scenarios, long-term operational evaluations, and repeatable benchmarking methodologies.

3.5.3. Explainability and Trustworthiness of Artificial Intelligence

DL models have achieved impressive detection performance; However, their limited interpretability remains a significant barrier to implementation in safety-critical environments. Security system operators require clear explanations to understand why threats are detected and why remediation is recommended. Existing XAI techniques provide only partial solutions and often involve a trade-off between interpretability and predictive performance. Developing trustworthy AI models that simultaneously demonstrate high accuracy, transparency, robustness, and regulatory compliance remains a significant research priority.

3.5.4. Adversarial Attack Resistance

While AI enhances cybersecurity, AI models themselves are increasingly becoming targets for attacks. Examples of adversarial attacks, data poisoning, model inversion, affiliation inference, and instant injection attacks can significantly degrade the reliability of autonomous security systems. The literature indicates a growing awareness of these threats; however, comprehensive defense mechanisms are still not fully developed. Future research should focus on robust learning algorithms, secure model update mechanisms, adversary training strategies, and continuous model validation to improve the resilience of AI-based cybersecurity platforms.

3.5.5. Scalability and Resource Awareness

Future CPS ecosystems will encompass millions of interconnected devices with widely varying computational capabilities and communication constraints. Many existing AI models require computational resources that exceed the capabilities of embedded IoT devices. Therefore, lightweight AI models, adaptive model compression, hardware-aware optimization, and energy-efficient learning algorithms require further research. Resource-aware, energy-efficient AI (Green AI) capable of dynamically adapting to changing computational conditions will be essential for sustainable autonomous security.

3.5.6. FL in Realistic Settings

FL has emerged as one of the most promising approaches to privacy protection in distributed cybersecurity. However, current research often assumes relatively stable communication networks and homogeneous participants. Practical implementations must consider data distribution other than Intelligent Intrusion Detection (IID), unreliable communication, client heterogeneity, asynchronous learning, and dynamic participation by edge devices. Furthermore, federated systems require stronger protection against model poisoning and Byzantine attacks. Future research should therefore explore adaptive aggre-

gation algorithms, secure collaboration protocols, incentive mechanisms, and robust trust management for large-scale industrial deployments.

3.5.7. GenAI for Autonomous Cyber Defense

GenAI has rapidly evolved from supporting security analysts to enabling automated threat intelligence generation, vulnerability assessment, attack simulation, and security policy support. However, its application in operational CPS environments remains in its early stages of development. Critical issues—such as hallucinations, explainability, instant injection attacks, model management, and verification of generated recommendations—must be addressed before GenAI can be safely integrated into autonomous cybersecurity processes. Future research should include domain-specific foundation models, secure instant engineering, search-assisted generation, and human-guided decision-making frameworks for protecting critical infrastructure.

3.5.8. DTs as Cybersecurity Platforms

DTs offer significant potential for continuous system monitoring, predictive risk assessment, attack simulation, and resilience assessment. However, current implementations primarily focus on operational optimization rather than cybersecurity. Furthermore, challenges related to real-time synchronization, interoperability, scalability, and secure communication between physical and virtual assets remain insufficiently addressed. Future work should include AI-enhanced digital twins capable of continuously assessing cyber threats, predicting attack propagation, and supporting autonomous response planning in CPS environments.

3.5.9. Standardization and Interoperability

The literature reveals a significant diversity of communication protocols, AI frameworks, data models, and security mechanisms used across CPS domains. This heterogeneity complicates the integration of autonomous security solutions across industry sectors and organizations. A greater emphasis is needed on interoperable architectures, standardized security interfaces, common evaluation methodologies, and open benchmarking datasets to facilitate technology transfer and objective comparison of proposed approaches.

3.5.10. Ethical, Regulatory, and Human-Centered Aspects

As AI assumes increasingly autonomous security responsibilities, technical performance alone is no longer sufficient. Future CPS security solutions must meet requirements for accountability, transparency, privacy, regulatory compliance, and human oversight. Human-mediated decision-making, AI governance, ethical risk assessment, and compliance with emerging AI and cybersecurity regulations should therefore become integral components of future autonomous security architectures, rather than secondary design considerations.

3.5.11. Towards a Self-Adaptive and Resilient CPS 2.0

The literature suggests a shift from reactive cybersecurity to intelligent, autonomous, and self-adaptive defense ecosystems. Instead of relying on isolated technologies, future CPS 2.0 security architectures will integrate AI/ML, FL, edge computing, GenAI, DTs, XAI, and zero-trust principles within collaborative and constantly evolving cyber defense platforms. Achieving this vision requires advances not only in AI algorithms but also in systems integration, interoperability, resilience, trust management, and validation under realistic operational conditions. Addressing these challenges will be fundamental to creating secure, scalable, and trustworthy CPS infrastructures capable of supporting the evolving requirements of Industry 5.0 and next-generation intelligent IoT ecosystems.

3.6. Economic Issues

The transition toward CPS 2.0 involves substantial initial investments in edge computing infrastructure, AI and ML systems, and FL platforms, which may present significant financial barriers, particularly for small and medium-sized enterprises (SMEs). In addition, the deployment and ongoing maintenance of distributed computing and security resources across multiple sites increase operational costs compared to traditional centralized architectures. The training and deployment of advanced AI and GenAI models further require high-performance hardware, resulting in higher energy consumption and the need for specialized processing units. Compliance with data privacy regulations also introduces additional costs, as organizations must implement secure FL protocols, auditing mechanisms, and governance frameworks. Moreover, integrating CPS 2.0 technologies into existing industrial workflows introduces economic risks related to system downtime, service interruptions, and operational disruptions [55].

The absence of standardized and interoperable platforms can further exacerbate costs by creating vendor lock-in effects, limiting flexibility and increasing long-term dependency on specific providers. At the same time, shortages of skilled professionals in AI, cybersecurity, and edge computing contribute to rising labor costs and slow down large-scale adoption. CPS 2.0 infrastructures are also exposed to cyber threats that may lead to direct financial losses through production outages, intellectual property theft, and ransomware attacks. Ongoing investments in system updates, model retraining, and adaptive security mechanisms are required to address evolving threats, placing continuous financial pressure on organizations [56]. Despite these challenges, CPS 2.0 has the potential to deliver long-term economic advantages through improved operational efficiency, reduced downtime, and enhanced system resilience, although the return on investment in the short term remains uncertain.

3.7. Social, Ethical and Legal Issues

CPS 2.0 raises significant societal concerns, particularly regarding potential job displacement as automation and AI-driven decision-making reduce the need for certain human roles. The increasing reliance on ML and GenAI can also create trust-related challenges, as users may find it difficult to interpret or validate how critical decisions are produced. Uneven access to CPS 2.0 technologies risks widening the digital divide, placing smaller enterprises, developing regions, and under-resourced organizations at a disadvantage. Ethical concerns become more pronounced when AI systems operate autonomously in safety-critical environments, particularly when their decisions result in unintended harm. In parallel, privacy risks intensify as large volumes of sensitive industrial, personal, and operational data are continuously generated and processed across distributed CPS networks [57].

Although FL supports data locality and privacy preservation, legal and regulatory frameworks must still address issues of accountability when model errors or biases propagate across distributed systems. The integration of GenAI into CPS 2.0 further introduces ethical risks, including the generation of misleading synthetic data, deepfakes, and adversarial manipulations that may influence system behavior. In addition, intellectual property rights become increasingly complex, as distributed AI models are jointly developed across multiple stakeholders without clearly defined ownership structures [58]. Social resistance may also emerge in response to pervasive monitoring and automation, particularly if employees perceive themselves as being excessively supervised or replaced by AI systems. Determining legal responsibility in CPS 2.0 environments is inherently challenging due to distributed decision-making processes involving multiple organizations, algorithms, and interconnected devices. The lack of transparency in advanced AI systems further

complicates regulatory compliance, as explainability is essential for ensuring accountability and adherence to legal and ethical standards. Cyberattacks on CPS 2.0 not only result in economic losses but can also pose serious risks to public safety, thereby increasing the ethical and legal obligations of system operators. Moreover, cross-border data flows enabled by federated learning introduce jurisdictional conflicts related to data sovereignty and international regulatory alignment [59]. Ultimately, public trust in CPS 2.0 deployment depends on transparent governance structures, responsible AI practices, and active societal engagement in policymaking. Addressing these social, ethical, and legal challenges requires adaptive regulatory frameworks, interdisciplinary oversight, and balanced approaches that align innovation with accountability.

3.8. Autonomous and Self-Healing CPSs

Autonomous and self-healing solutions in CPS 2.0 in IoT ecosystems refer to advanced architectures that enable systems to automatically manage, adapt, and self-heal in response to anomalies or cyberthreats. These solutions are increasingly driven by AI-based autonomous security mechanisms that continuously monitor system behavior across distributed IoT nodes. In CPS 2.0, self-healing is implemented through closed-loop control systems that integrate real-time detection, analytics, and automated actions [60]. ML models, particularly anomaly detection and reinforcement learning, are used to identify deviations from normal operating patterns. When a threat or fault is detected, autonomous mechanisms trigger mitigation strategies, such as isolating infected nodes, reconfiguring network routes, or restoring corrupted firmware. These capabilities reduce human intervention and significantly improve system resilience in large-scale IoT environments. Self-healing platforms also leverage DTs to simulate system states and predict optimal remediation actions before deployment [61]. AI-powered orchestration layers coordinate security policies across heterogeneous devices, ensuring consistent enforcement even under dynamic conditions. In CPS 2.0, autonomy goes beyond reactive defense to proactive defense, where predictive analytics anticipate attacks and preemptively shore up vulnerabilities [62]. These autonomous and self-healing solutions provide the foundation for secure, scalable, and resilient IoT ecosystems in next-generation cyber–physical infrastructures (Figure 8).

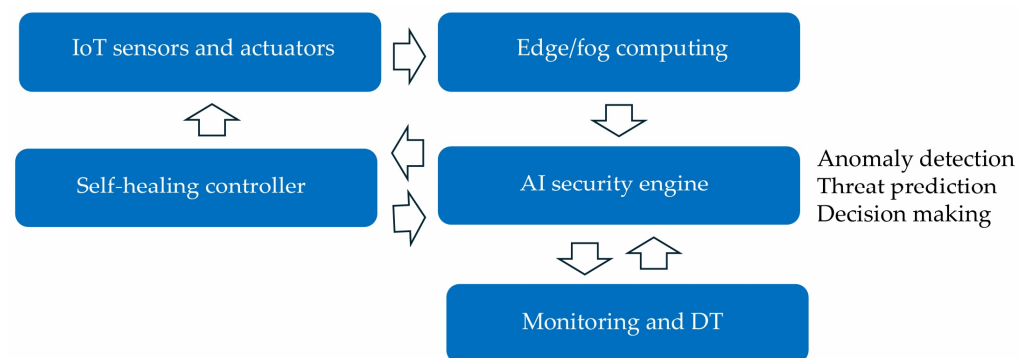


Figure 8. Autonomous and self-healing structure of CPS 2.0.

3.9. Co-Operation of CPS 2.0 Within Industry 6.0

CPS 2.0 is based on intelligent collaboration between humans, machines, AI agents, and connected IoT devices operating in highly adaptive environments. Autonomous AI-driven security enables these entities to securely exchange data, coordinate actions, and maintain trust in distributed industrial ecosystems. CPS 2.0 architectures leverage machine learning algorithms to facilitate real-time decision-making while continuously monitoring for cyberthreats and operational anomalies. Autonomous collaboration is implemented through secure machine-to-machine (M2M) communication protocols that support dy-

dynamic resource sharing and coordinated task execution [63]. DTs enhance collaboration by providing virtual representations of physical assets, enabling predictive analytics and synchronized responses between system components. In Industry 6.0 environments, AI-driven security agents collaborate across the edge, fog, and cloud layers to detect, assess, and mitigate cyberattacks with minimal human intervention. Self-organizing CPS 2.0 networks can dynamically reconfigure communication paths and operational workflows to maintain service continuity in the event of disruption. Collaborative security frameworks leverage federated learning and distributed intelligence, enabling multiple devices to learn from shared experiences without exposing sensitive data. Human-centric design principles enable transparent collaboration between autonomous systems and operators, enabling meaningful security decisions and providing human oversight when needed [64]. Industry 6.0 Collaboration: CPS 2.0 combines autonomous intelligence, resilient security mechanisms, and connected IoT infrastructures to create secure, adaptive, and sustainable infrastructures (Figure 9).

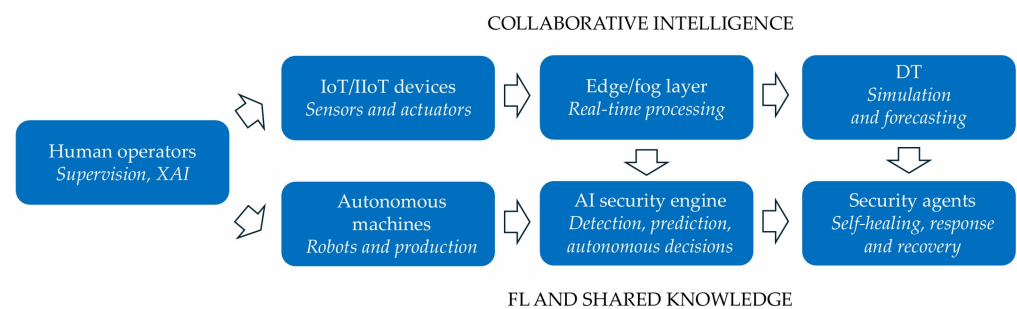


Figure 9. Role of CPS 2.0 within Industry 6.0 paradigm.

3.10. Advantages and Weaknesses of Autonomous CPS 2.0

CPS 2.0 enables real-time decision-making through the integration of edge computing, which reduces latency and improves responsiveness in time-critical applications. The incorporation of AI, ML, and GenAI strengthens predictive analytics, supports anomaly detection, and enhances adaptive defense mechanisms against evolving cyber threats. FL further contributes by enabling collaborative model training without the exchange of raw data, thereby improving privacy protection and supporting regulatory compliance. The decentralized nature of the CPS 2.0 architecture also enhances system resilience by eliminating single points of failure that are typical in centralized systems. In addition, digital twin technologies and simulation environments allow safe testing and optimization of system behaviors before deployment in real-world conditions. However, the increasing reliance on advanced AI systems introduces challenges related to model interpretability, making it difficult to explain, justify, or validate automated decisions [65].

At the same time, edge computing and federated learning environments are constrained by limited computational resources, communication overhead, and variability in data quality across distributed nodes. The integration of multiple advanced technologies further increases system complexity and raises significant interoperability challenges, often requiring expensive standardization efforts. Security risks also persist, as federated learning and GenAI models remain susceptible to adversarial attacks, data poisoning, and manipulation attempts [66]. While CPS 2.0 provides improved adaptability, scalability, and operational efficiency, these advantages are accompanied by new challenges related to system complexity, operational cost, and secure management of highly distributed intelligent infrastructures.

Mitigation strategies in CPS 2.0 are primarily grounded in a zero-trust security model that enforces continuous authentication and authorization for all devices, users, and applications. Edge intelligence reduces dependence on centralized servers, thereby lowering

latency risks and enabling rapid local responses to cyber incidents. FL is employed as a privacy-preserving mechanism that limits exposure of raw data while improving the robustness of global security models. In addition, adversarial training and continuous model validation are used to strengthen AI and GenAI systems against data poisoning, evasion, and manipulation attacks. Redundant, fault-tolerant system architectures further ensure operational continuity even under cyberattacks or system failures [67]. Continuous monitoring and anomaly detection mechanisms provide early warning capabilities by identifying abnormal behavior before it escalates into major disruptions.

In application domains, CPS 2.0 enhances predictive maintenance in industrial control systems, enabling earlier detection of equipment degradation and reducing operational downtime. In smart manufacturing environments, it supports optimized production processes while maintaining resilience against cyber-physical threats. In power grid systems, CPS 2.0 facilitates real-time load balancing and intrusion prevention, thereby safeguarding critical energy infrastructure from failures and malicious interference. In transportation systems, it enables autonomous vehicle coordination and intelligent traffic management, where integrated risk mitigation strategies are essential to ensure both functional safety and cybersecurity.

3.11. Conceptual Roadmap for Developing Resilient, Secure, and Privacy-Preserving Autonomous CPS 2.0 Infrastructure Prepared for Industry 6.0

Building on our proposed concept, we begin by adopting a zero-trust architecture as the foundational security paradigm, ensuring continuous authentication and verification of all devices, services, and users [68]. To strengthen privacy while preserving operational efficiency, we integrate end-to-end encryption alongside data minimization techniques. A decentralized network of redundant edge computing nodes is established to reduce latency, enhance system resilience, and maintain continuity of operations during potential network disruptions. AI-driven anomaly detection mechanisms are incorporated to enable real-time identification of cyber-physical threats and to support adaptive responses that prevent cascading system failures. Blockchain and distributed ledger technologies are utilized to secure machine-to-machine interactions, improve traceability, and ensure data integrity across interconnected supply chains. DT and simulation environments are developed to continuously evaluate CPS infrastructures under cyber, physical, and hybrid threat scenarios.

Furthermore, system design emphasizes modular and interoperable components, allowing seamless updates and security patches without interrupting critical operations. Privacy-enhancing technologies (PETs), including FL and secure multi-party computation, are implemented to enable collaborative intelligence without exposing sensitive data. Human-centric governance frameworks are introduced to balance automation with ethical oversight, ensuring transparency, accountability, and trust in decision-making processes. Self-healing capabilities are embedded within CPS 2.0 components to enable automatic reconfiguration, rerouting, and recovery from faults or cyber incidents. In parallel, cross-sector standards and compliance frameworks are advocated to harmonize security and resilience requirements across industries and geographic regions.

The next phase involves the development of real-time situational awareness dashboards that integrate cyber, physical, and human data streams to support rapid and informed decision-making [69–74]. This approach also incorporates ecological and sustainable design principles to ensure alignment with Industry 5.0 priorities, particularly human-machine collaboration and environmental responsibility [75–78]. Looking ahead, the vision extends toward cognitive CPS 2.0 ecosystems characterized by context-aware, adaptive, and predictive interactions between humans and machines [79]. Continuous lifelong learning mechanisms are essential to enable ongoing evolution of CPS 2.0 infrastruc-

ture, ultimately supporting the transition toward Industry 6.0, defined by hyper-intelligent, autonomous, and globally interconnected systems. Table 9 presents a five-layer CPS 2.0 ecosystem in which governance defines operational rules, technology provides the foundational infrastructure, security ensures trust and resilience, the human layer enables collaboration, and sustainability ensures long-term system viability.

Table 9. Layered structure of a resilient, secure, and privacy-aware autonomous CPS 2.0 (own elaboration).

Layer Name	Functions
Governance and strategy	Zero-trust principles should serve as a mandatory benchmark across all industries. Cross-sector standards, regulatory compliance frameworks, and international cooperation should promote interoperability. Ethical oversight mechanisms must ensure integrity, transparency, and accountability, while sustainability-focused regulations should align with the values and objectives of Industry 5.0 [80,81].
Security and privacy	End-to-end encryption and data minimization should be implemented as default configurations. AI-driven threat intelligence and anomaly detection capabilities should enable proactive cybersecurity defenses. Self-healing mechanisms should support automatic recovery from disruptions, while PETs, including FL, should facilitate secure and privacy-preserving collaboration [82,83].
Organization and human-centricity	Human-centered management approaches should balance system autonomy with appropriate human oversight. Operator dashboards should provide real-time situational awareness to support informed decision-making. Interdisciplinary training programs should bridge the human, cyber, and physical domains, fostering integrated expertise. In addition, a culture of ethical design should guide innovation and the implementation of CPS, ensuring responsible and sustainable development [84,85].
Technology and infrastructure	Modular and interoperable architectures should be adopted to enhance scalability, flexibility, and seamless system integration. Edge and fog computing nodes should support low-latency operations and improve system resilience. Blockchain and distributed ledger technologies should enable secure and trustworthy data exchange among machines, while digital twins should facilitate predictive monitoring, simulation, and stress testing to optimize performance and reliability [86–88].
Sustainability and readiness for development	Energy-efficient and sustainable infrastructures, including Green AI technologies, should be designed to minimize environmental impact. Adaptive and cognitive CPS ecosystems should continuously learn, evolve, and respond to changing operational contexts. Lifelong learning mechanisms should enable ongoing improvement and readiness for the transition toward Industry 6.0. Furthermore, resilient global collaborative networks should promote inclusivity, innovation, and long-term economic sustainability [88,89].

4. Discussion

CPS 2.0 represents the next evolution of digital–physical integration, bringing together edge computing, AI, GenAI, and FL to support the development of resilient, adaptive, and intelligent infrastructures aligned with Industry 4.0 and Industry 5.0 paradigms. In contrast to conventional centralized architectures, CPS 2.0 prioritizes decentralized system

designs that better address challenges related to latency, scalability, and data sensitivity [90]. However, these technological advancements also introduce a wide range of challenges spanning technical, economic, social, ethical, and legal dimensions [91–94].

The revised taxonomy classifies AI-based cybersecurity capabilities according to their functional roles in the CPS 2.0 security lifecycle, rather than individual technologies. The first layer, intelligent detection and monitoring, focuses on the continuous collection, aggregation, and pre-processing of data from sensors, IoT devices, and cyber-physical assets to provide comprehensive situational awareness. The second layer, distributed learning and privacy protection, encompasses techniques such as FL, edge intelligence, and privacy-enhancing methods that enable collaborative model training without exposing sensitive data. The third layer, AI-based threat detection and prediction, leverages ML, DL, and GenAI to identify anomalies, recognize attack patterns, predict emerging threats, and support cybersecurity decision-making. The fourth layer, autonomous response and recovery, encompasses AI-based mechanisms that automatically select and implement mitigation strategies, isolate infected components, and restore normal system operation with minimal human intervention. The fifth layer, continuous adaptation and system resilience, enables cybersecurity models to learn from operational feedback, adapt to evolving attack strategies, and improve long-term resilience and reliability. These functional layers create an integrated security workflow in which information and decisions continuously flow from monitoring to learning, prediction, response, and adaptation. Unlike technology-centric classifications, this taxonomy highlights the operational roles AI plays throughout the cybersecurity lifecycle. It also illustrates how multiple technologies—including edge computing, FL, DTs, and GenAI—interact within each functional layer to provide adaptive defense. Therefore, the proposed taxonomy highlights the evolution of CPS cybersecurity from static, reactive defense mechanisms toward intelligent, autonomous, and resilience-focused security architectures characteristic of CPS 2.0.

From a technical perspective, limitations include constrained resources, interoperability difficulties, and increased exposure to cyberattacks, while economic challenges arise from substantial investment requirements, high operational costs, and increased demand for specialized expertise [95,96]. At the same time, social and ethical concerns are becoming more prominent, particularly in relation to employment shifts, governance structures, privacy protection, and accountability. Legal complexities are also emerging, especially regarding cross-border data exchange and the attribution of responsibility in distributed decision-making systems [97,98]. Despite these challenges, CPS 2.0 offers significant advantages, including real-time threat detection, predictive maintenance, improved system resilience, and privacy-preserving collaboration enabled by federated learning [99]. Effective risk mitigation strategies include zero-trust security models, adversarial training, system redundancy, continuous monitoring, and the use of digital twin environments for simulation-based security testing and validation [100]. Real-world applications in domains such as industrial control systems, energy networks, and transportation infrastructures highlight both the transformative potential and the associated risks of CPS 2.0 deployment [101]. In next study, authors proposed a framework for assessing the resilience of cyber-physical power systems (CPPSs) that covers the entire lifecycle of cyberattacks in modern smart grids. This framework models the attack success probability using a Markov node transition probability matrix with a depth-first search algorithm, while a mixed, non-sequential Monte Carlo simulation determines the occurrence and recovery time of circuit breaker failures. To represent the operational impact of successful cyberattacks, the authors developed a power system response model based on optimal load shedding using direct current flow and introduced four resilience metrics that assess attack resilience, system adaptability, recovery capacity, and overall resilience. The proposed methodol-

ogy was validated through simulations on the IEEE RTS 79 test system, demonstrating its effectiveness in assessing the resilience of CPPSs in cyberattack scenarios [102]. Next study examines the limitations of conventional power line hardening strategies, taking into account the uncertainty and multi-stage nature of malicious attacks, as well as the operational variability introduced by high wind power penetration. To improve defense planning, the authors propose an adaptive, resilient Adaptive Reliability Planner-Attacker-Operator (AR-PAO) model that integrates uncertain attack scenarios and variable wind power generation into the power line hardening framework, supported by an efficient solution algorithm. Validation on two IEEE Reliability Test Systems demonstrates that the proposed approach effectively improves defense strategy optimization under uncertain cyber-physical operational conditions [103].

The successful implementation of CPS 2.0 requires a balanced integration of technological innovation, robust regulatory frameworks, and international collaboration to ensure secure, trustworthy, and sustainable operation in critical infrastructure systems. To summarize the review and analysis results, we address the RQs:

1. RQ1: In CPS 2.0, the following AI-based autonomous security approaches have been proposed and implemented in IoT ecosystems:
 - AI-based intrusion detection systems (IDSs) are widely used to develop autonomous intrusion detection systems for CPS 2.0. These systems analyze network traffic, device behavior, and communication patterns to identify malicious activity in real time. Popular approaches include support vector machines (SVMs), random forests, convolutional neural networks (CNNs), and long short-term memory networks (LSTMs), which can detect both known and previously unseen cyberattacks.
 - Autonomous anomaly detection establishes normal operational baselines for cyber-physical processes and IoT devices. Using unsupervised and semi-supervised learning algorithms, these systems autonomously identify anomalous behaviors that may indicate cyberattacks, hardware failures, or insider threats. These approaches are particularly valuable in dynamic CPS environments where attack signatures may be unavailable.
 - Adaptive security based on machine learning (reinforcement learning) enables CPS 2.0 systems to autonomously learn optimal security strategies through continuous interaction with the environment. RL-based security frameworks can dynamically adjust access controls, network configurations, and defenses to minimize security risks while maintaining operational efficiency.
 - AI-based threat intelligence and prediction predictive AI models analyze historical security events, threat sources, and system logs to predict potential cyberthreats before they occur. These approaches leverage machine learning algorithms to identify attack patterns, assess risk levels, and provide proactive mitigation recommendations in IoT-enabled CPS environments.
 - AI-based autonomous malware and botnet detection are increasingly being used to identify malware infections and botnet activity targeting IoT devices. Deep learning models can analyze executable behavior, communication flows, and device interactions to automatically detect malware, even when attackers employ obfuscation techniques.
 - FL for privacy-preserving security enables distributed CPS and IoT devices to jointly train AI security models without sharing raw data. This approach enhances privacy, reduces centralized vulnerabilities, and supports scalable security intelligence in geographically distributed CPS 2.0 environments while maintaining data confidentiality.

- AI-based access control and authentication are used to develop adaptive authentication mechanisms and intelligent access control. These systems continuously evaluate user behavior, device trustworthiness, contextual information, and risk factors to autonomously grant, restrict, or revoke access, thereby strengthening CPS security against unauthorized access.
 - Self-healing and autonomous cyber defense systems represent an advanced form of AI-based autonomous defense in CPS 2.0. These systems automatically detect attacks, isolate infected components, restore affected services, and reconfigure network resources without human intervention. This approach increases cyber resilience and ensures the continuity of critical IoT-enabled infrastructures.
2. RQ2: AI-based autonomous security in CPS 2.0 in IoT ecosystems introduces a shift from reactive, human-driven defense mechanisms to intelligent, adaptive, and continuously learning defense architectures. Evidence from the recent literature highlights a clear balance between significant benefits and equally significant technical, organizational, and societal constraints. The main benefits are primarily related to improved real-time security intelligence and scalability. AI, combined with edge computing and FL, enables continuous monitoring, rapid anomaly detection, and autonomous response to cyber threats without relying on centralized infrastructure. This significantly reduces latency and improves resilience in large-scale IoT environments. FL further enhances privacy by enabling collaborative model training without sharing raw data, which is particularly important in sensitive areas such as healthcare, smart grids, and transportation. Generative AI models also enhance security's predictive capabilities, enabling early detection of complex or evolving attacks, including zero-day threats. Furthermore, distributed architectures increase fault tolerance by eliminating single points of failure and supporting self-healing and adaptive defense mechanisms. Despite these advantages, several key challenges remain. One major issue is resource constraints at the network edge, where limited computing power, memory, and energy hinder the deployment of advanced AI models. Communication overhead in federated learning systems, along with model drift and inconsistent data quality across distributed nodes, can degrade performance. Interoperability between heterogeneous devices and platforms in CPS 2.0 and IoT ecosystems also remains unresolved, requiring standardization efforts. Security threats persist even in AI-based systems, as adversarial attacks, data poisoning, and model manipulation can target both centralized and distributed learning processes. Furthermore, explainability remains a significant challenge, as autonomous decisions made by AI are often difficult to interpret or justify in safety-critical environments. Key limitations occur at the technical, economic, and managerial levels. High implementation costs associated with edge infrastructure, AI/GenAI models, and federated learning platforms limit adoption, particularly among small and medium-sized enterprises. Legal and regulatory uncertainty surrounding cross-border data flows, accountability in distributed decision-making, and compliance with privacy regulations further complicates implementation. Increased automation, including job displacement, surveillance risks, and limited human oversight of key decisions, further complicate ethical issues. Furthermore, the lack of a mature, standardized framework for integrating AI, federated learning, blockchain, and edge computing limits interoperability at scale and slows practical implementation. AI-based autonomous security in CPS 2.0 offers revolutionary improvements in real-time threat detection, privacy protection, and system resilience, but its effectiveness is limited by limited resources, AI model vulnerabilities, interoperability gaps, and unresolved ethical and regulatory issues.

3. RQ3: New AI techniques are playing a key role in enabling autonomous security capabilities in CPS 2.0 in IoT ecosystems, transforming how threats are detected, mitigated, and managed in real time. In the literature, AI is consistently positioned as a foundational intelligence layer that shifts cybersecurity from a rule-based and reactive approach toward predictive, adaptive, and self-organizing defense mechanisms. In autonomous threat detection, machine learning and deep learning models enable continuous monitoring and analysis of large amounts of heterogeneous data generated by IoT devices. These techniques can identify complex patterns, detect anomalies, and recognize previously unobserved attack behaviors such as zero-day exploits, advanced persistent threats, and data poisoning attempts. Deployed at the edge, AI models significantly reduce detection latency by processing data close to its source, while federated learning enables distributed training across multiple nodes without exposing the raw data, improving both scalability and privacy. GenAI further enhances detection by simulating attack scenarios and enriching training datasets, improving model resilience in data-poor or imbalanced environments. In terms of threat mitigation, AI-based systems support automated and context-aware response mechanisms. When anomalies are detected, reinforcement learning and adaptive AI models can trigger dynamic countermeasures such as traffic redirection, access revocation, workload isolation, or system reconfiguration. In federated and edge architectures, these responses can be executed locally, reducing reliance on centralized decision-making and improving response speed. Blockchain-integrated AI frameworks further enhance threat mitigation by providing secure authentication, tamper-proof logging, and trusted coordination between distributed CPS 2.0 components. In terms of system resilience, AI contributes to system resilience by enabling self-healing, predictive maintenance, and continuous adaptation to changing operational and cybersecurity conditions. Predictive analytics can predict system failures or security breaches before they occur, enabling proactive interventions that reduce downtime and improve reliability. Digital twin environments combined with AI also enable continuous simulation and validation of security strategies across various threat scenarios, increasing preparedness and reliability. Federated learning increases resilience by distributing data across the network, ensuring that even if individual nodes are compromised or go offline, the entire system continues to function securely. Modern AI techniques (including DL, FL, RLGenAI, and edge intelligence) collectively enable CPS 2.0 systems to transition to autonomous cybersecurity paradigms. These techniques improve detection accuracy, shorten response times, and strengthen system resilience, while enabling privacy protection and scalable security operations in complex IoT ecosystems.
4. RQ4: Research on AI-based autonomous security in CPS 2.0 and IoT ecosystems has made significant progress, but the literature consistently identifies several significant gaps that limit current capabilities and shape future directions:
 - A major research gap concerns the resilience of AI models under attack. While machine learning, federated learning, and generative AI are improving detection and response capabilities, they remain vulnerable to attacks such as data poisoning, unwinding, and model inversion. Existing defenses are still not sufficiently robust in security-critical CPS environments, especially when attacks target distributed learning pipelines at the network edge.
 - Another key gap lies in the lack of explainability and reliability of autonomous security decisions. Many AI-based intrusion detection and response systems operate as “black boxes,” making it difficult for operators to interpret or verify decisions in real time. This limits their implementation in regulated domains such

as healthcare, energy, and transportation, where accountability and transparency are essential.

- Another limitation is the limited resources for deployment in edge and IoT environments. CPS 2.0 systems rely heavily on edge devices with limited computational power, memory, and energy capacity, limiting the use of complex AI and generative models. Efficient, lightweight, and adaptive AI architectures remain underdeveloped, especially for large-scale, heterogeneous IoT deployments.
- There is also a significant gap in interoperability and standardization within CPS 2.0 ecosystems. Current solutions often operate in isolated environments with limited compatibility between federated learning platforms, edge platforms, blockchain systems, and AI security modules. This fragmentation hinders large-scale integration and real-world deployment.
- From a data perspective, challenges remain in handling non-IID (independent and identically distributed) and imbalanced data across distributed nodes, which negatively impacts model convergence and accuracy in federated learning-based security systems. Furthermore, issues such as model drift, inconsistent data quality, and unreliable labeling continue to limit performance in dynamic IoT environments.
- Several research directions are emerging. First, there is a strong need for robust and attack-resistant AI frameworks, including hybrid defense mechanisms combining federated learning, adversary training, and blockchain-based trust management. Second, research should focus on explainable and eXplainable (XAI) for CPS security, enabling transparent decision-making and validation with human input. Third, the development of lightweight and energy-efficient AI models for edge devices is essential to ensuring real-time security in resource-constrained environments.
- Future work should also emphasize fully integrated CPS 2.0 security architectures, where AI, FL, edge computing, and DTs operate in a unified orchestration framework with standard protocols. Furthermore, privacy-preserving collaborative learning techniques, such as enhanced federated learning with differential privacy and secure aggregation, should be further optimized for scalability and reliability. Research is also expected to evolve toward self-healing, autonomous, and cognitive CPS ecosystems, where systems continuously learn, adapt, and recover from attacks with minimal human intervention.
- The field is moving toward highly autonomous, distributed, and intelligent security frameworks, but achieving this vision requires overcoming key challenges in reliability, transparency, interoperability, and scalability in real-world settings.

The discussion should go beyond describing cybersecurity mechanisms and emphasize the fundamental relationship between security, resilience, autonomy, and the convergence of the cyber and physical domains in CPS 2.0. CPSs tightly integrate computational intelligence, communication networks, sensor infrastructure, and physical processes, creating highly interconnected environments in which cybersecurity incidents can rapidly spread, leading to physical disruptions with security, operational, and economic consequences. Unlike traditional IT systems, CPS security must simultaneously protect digital assets, maintain the integrity of physical processes, and maintain real-time operational continuity despite failures, malware attacks, or unpredictable environmental conditions. Consequently, the concept of resilience has become a complementary goal to conventional cybersecurity, emphasizing the ability of a CPS not only to prevent attacks but also to anticipate threats, counter disruptions, adapt to changing conditions, quickly recover, and continuously improve its defensive capabilities. This evolution reflects the growing

realization that complete prevention of sophisticated cyberattacks is impractical in vast IoT-based infrastructures characterized by heterogeneous devices, distributed control architectures, dynamic topologies, and expanding attack surfaces. The increasing adoption of edge computing, cloud-native services, software-defined networks, DTs, and autonomous decision-making further complicates security management by introducing additional dependencies, trust relationships, and potential vulnerabilities across multiple computational layers. At the same time, the rapid development of AI poses a dual challenge: AI techniques significantly improve threat detection, anomaly identification, adaptive risk assessment, and automated incident response, while AI models themselves become attractive targets for manipulation, data poisoning, model inversion, and privacy attacks. Achieving reliable CPS operation therefore requires security mechanisms capable of continuously assessing system health, correlating heterogeneous data sources, reasoning under uncertainty, and autonomously selecting mitigation strategies without compromising real-time security or constraints. These requirements have accelerated the shift from static, rule-based security architectures to cognitive and autonomous cybersecurity frameworks that integrate ML, reinforcement learning, FL, GenAI, and XAI into continuous monitoring and decision support. From a resilience perspective, effective CPS protection goes beyond intrusion detection to encompass adaptive system reconfiguration, fault isolation, self-healing, predictive maintenance, and coordinated recovery mechanisms that minimize cascading failures across interconnected cyber and physical components. Therefore, security and resilience should be viewed as mutually reinforcing properties within CPS 2.0, where AI-based autonomous defense architectures provide the insights necessary to maintain the reliable, robust, and resilient operation of increasingly complex IoT ecosystems operating in dynamic and aggressive environments.

4.1. Limitations

The review is limited by the selection of scholarly databases, which may have excluded relevant studies indexed elsewhere. The search strategy, including the selection of keywords and inclusion criteria, may have influenced the scope of emerging or interdisciplinary research on AI-based cybersecurity in the context of CPS 2.0 and IoT. The search strategy required the use of the term “autonomy” in the primary search string, which may have excluded relevant studies addressing autonomous cybersecurity concepts without explicitly using this terminology, thereby introducing a degree of selection bias. This potential bias was mitigated by backward and forward citation tracking, manual selection of highly relevant publications, and expert judgment during narrative synthesis; however, it cannot be considered completely eliminated. Only peer-reviewed publications in English were included, potentially introducing linguistic and publication bias while simultaneously excluding the valuable gray literature and industry reports. As a narrative review, the study does not fully utilize formal bibliometric methodology, a systematic review protocol, or quantitative meta-analysis, limiting an objective assessment of publication trends, citation networks, and research impact. The synthesis and interpretation of the selected literature inevitably involve a degree of authorial judgment, which may influence the relative emphasis placed on particular technologies or research directions. Therefore, the results should be interpreted as a qualitative synthesis of the current state of knowledge rather than a statistically comprehensive representation of the entire research landscape.

We examined the limitations associated with the proposed CPS 2.0 infrastructure roadmap. The large-scale deployment of zero-trust architectures and advanced cryptographic mechanisms may introduce substantial computational overhead and increased latency, particularly in real-time CPS 2.0 environments. Similarly, AI-based anomaly detection systems are subject to inaccuracies, where false positives or false negatives may

either disrupt normal operations or fail to identify sophisticated threats. The integration of blockchain technologies also presents challenges related to scalability, energy consumption, and interoperability, especially in high-throughput, low-latency industrial contexts. Digital twin and simulation-based approaches require considerable computational resources, domain expertise, and high-fidelity system modeling, which may not fully capture real-world complexity [103,104]. In addition, privacy-preserving techniques such as FL are still in relatively early stages of maturity, limiting their widespread adoption across heterogeneous CPS 2.0 environments. The establishment of global standards and unified governance frameworks is further constrained by geopolitical factors, regulatory divergence, and uneven levels of regional implementation. The deployment of self-healing and adaptive mechanisms increases overall system complexity, which may introduce unintended behaviors or new security vulnerabilities [105]. The proposed roadmap also assumes the availability of highly skilled professionals in cybersecurity, artificial intelligence, and CPS 2.0 engineering—an assumption that may not align with current labor market constraints. Furthermore, sustainability objectives may conflict with industrial priorities focused on cost efficiency and operational performance, limiting their practical adoption. Finally, efforts to prepare for the highly autonomous ecosystems envisioned in Industry 6.0 may risk overly speculative system designs, as future technological and societal trajectories remain uncertain and require careful mitigation strategies (Table 10).

Table 10. Proposed strategies for addressing existing limitations to enhance the sustainability and practical applicability of the autonomous CPS 2.0 roadmap (author’s own elaboration).

Constraint	Proposed Way of Mitigating
Zero-trust and cryptography overhead	Lightweight cryptographic techniques, such as elliptic curve cryptography (ECC) and post-quantum optimized algorithms, should be integrated to enhance security while minimizing computational overhead. Hardware accelerators should further improve processing efficiency, reducing latency and supporting the real-time performance requirements of CPS.
AI anomaly detection errors	Hybrid approaches that integrate rule-based methods with AI-driven detection should be employed, complemented by periodic human validation to minimize false positives and false negatives.
Blockchain scalability challenges	Permissioned blockchains or Layer 2 scaling solutions, such as sidechains and sharding, should be implemented to enhance transaction throughput while improving energy efficiency.
DT complexity	Begin with partial or modular digital twins centered on critical assets, then progressively expand the models by incorporating feedback from operational data.
Immaturity of PETs	Hybrid approaches that integrate PETs with traditional anonymization techniques should be adopted, alongside phased pilot implementations to progressively build and mature capabilities over time.
Incompatibility with global governance	Regional standardization efforts should be prioritized initially, with a focus on developing interoperable bridges rather than pursuing immediate global uniformity.
Complexity of self-healing mechanisms	Systems should be designed with security-by-default principles and multi-layered recovery mechanisms, ensuring that self-healing processes do not override or compromise critical security constraints.
Staff shortages	Interdisciplinary training programs should be established, supported by AI-driven development tools, and reinforced through public–private partnerships to accelerate skills development.

Table 10. Cont.

Constraint	Proposed Way of Mitigating
Sustainability vs. efficiency	A dual-optimization strategy should be adopted to balance high-throughput operations with eco-friendly scheduling, energy-efficient equipment usage, and circular economy principles.
Uncertainty about the future of Industry 6.0	Flexible, modular architectures should be implemented to support adaptation to diverse future scenarios while avoiding overinvestment in speculative or uncertain projects.

4.2. Direction of Further Research

The research directions presented below (Table 11) are intended to support the development of an autonomous CPS 2.0 infrastructure that is not only technically resilient, but also ethically governed, human-centered, and environmentally sustainable.

Table 11. Main research directions (own elaboration).

Area of Research	Detailed Description
Lightweight security protocols for CPS	Cryptographic and authentication mechanisms should be developed and optimized for real-time, resource-constrained environments while maintaining strong resilience and security [106].
AI for adaptive cyber–physical defense	Explainable, self-learning, and context-aware AI models should be developed to detect and respond to hybrid cyber–physical attacks while reducing false positives [107].
Privacy-preserving collaborative frameworks	FL, homomorphic encryption, and secure multi-party computation should be extended to support cross-industry data sharing without exposing sensitive information [108].
Blockchain and beyond for CPS trust	Scalable and energy-efficient distributed ledger technologies (DLTs) and consensus mechanisms should be explored and tailored to industrial machine-to-machine ecosystems [109].
DTs resilience modeling	Multi-scale, real-time digital twins should be developed to simulate not only physical and cyber disruptions but also interactions among humans and the environment within the context of Industry 5.0 and Industry 6.0 [110].
Self-healing and autonomous CPS systems	Architectures should be explored that integrate redundancy, AI-driven data recovery, and human oversight to maintain the stability of safety-critical systems during failures [111].
Governance and standardization models	Adaptive policy frameworks and interoperability standards should be developed to balance global harmonization with local regulatory, cultural, and ethical requirements [112].
Novel human–machine collaboration paradigms	Cognitive, ergonomic, and ethical interfaces should be developed to ensure that humans retain decision-making authority within increasingly autonomous CPS ecosystems [113].
Sustainable/ecological CPS systems	Energy-efficient architectures, circular economy strategies, and carbon-neutral design principles should be explored to align CPS 2.0 with the sustainability goals of Industry 5.0 [114].
Future-proof CPS systems for Industry 6.0	Architectures should be explored that can evolve into highly intelligent, globally connected systems while prioritizing resilience against unknown and emerging threats [115].

The thematic groupings presented in Figure 10 provide a structured way to organize the content, illustrating how technical, human, governance, and sustainability dimensions are interconnected and collectively shape the prioritization of research and implementation activities [116].

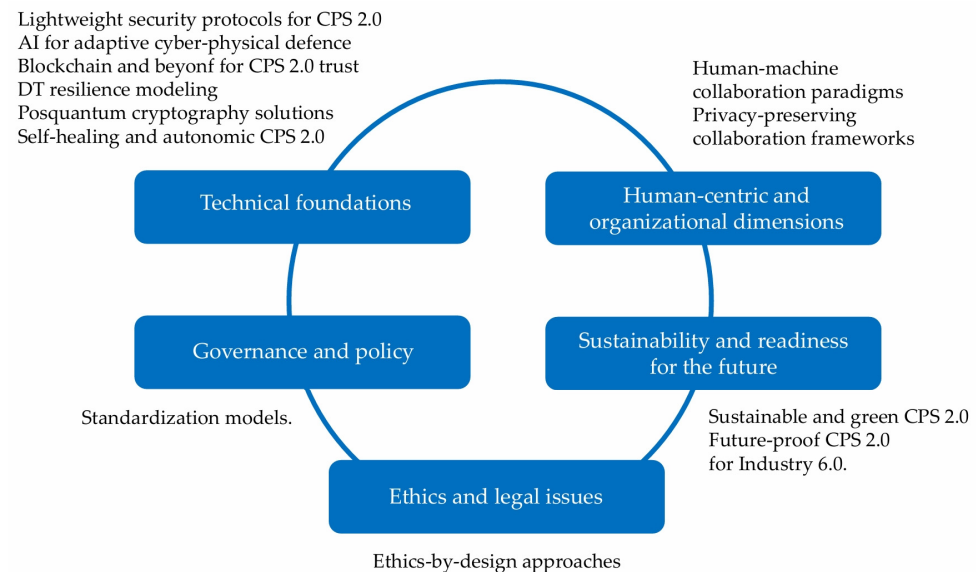


Figure 10. Cluster-based overview of the main research directions for resilient, secure, and privacy-preserving CPS 2.0 s (own elaboration).

The future research agenda for autonomous security in CPS 2.0 focuses on transforming cybersecurity from reactive defense mechanisms to proactive, adaptive, and self-evolving defense ecosystems. A key research direction is the development of cyberphysics-based security models capable of understanding the complex interactions between cyberattacks and their potential physical consequences [117]. Future systems should integrate DTs, physics-based AI, and cyber-physical attack graphs to enable accurate risk assessment and impact prediction [118]. Another key area is securing the communication infrastructure connecting IoT devices, edge nodes, and cloud platforms against interception, manipulation, and availability attacks [119]. Research should include adaptive network protection mechanisms, zero-trust architectures, and lightweight security protocols suitable for large-scale, resource-constrained CPS environments. The security and trustworthiness of AI models pose significant challenges, requiring robust approaches to protect against adversarial attacks, data poisoning, model manipulation, and unreliable autonomous decisions [120]. Future AI-based security frameworks should incorporate XAI, secure FL, and continuous model validation to ensure transparency, reliability, and accountability [121]. A resilience-focused CPS 2.0 design should go beyond attack prevention to enable systems to detect, adapt, recover, and maintain critical operations during cyber disruptions [122]. Self-healing architectures, autonomous recovery strategies, and reinforcement learning-based security policies are promising approaches to achieving adaptive resilience [123]. Privacy-preserving intelligence will remain essential, requiring advanced federated learning, differential privacy, and secure collaborative learning mechanisms in distributed CPS environments [124]. Human-AI collaboration should also be explored to establish appropriate levels of oversight, decision support, and governance for autonomous cybersecurity operations. Future research must address the standardization, certification, and regulatory challenges associated with implementing AI-based autonomous security in safety-critical CPS applications. The integration of GenAI, edge computing, federated intelligence, and DTs is expected to create more context-aware and adaptive cybersecurity ecosystems [125]. A key goal is to

develop CPS 2.0 architectures capable of continuous learning and autonomous adaptation to evolving cyberthreats [126]. This roadmap outlines a path to secure, scalable, privacy-aware, and resilient CPS 2.0 infrastructures supporting future Industry 4.0 and Industry 5.0 applications [127–129]. Structured research trajectory for CPS 2.0 autonomous security development is presented in Table 12.

Table 12. Research Roadmap for Autonomous Security in CPS 2.0.

Research Area	Current Limitations	Future Research Objectives	Enabling Technologies
Cyber–physical security modeling	Limited understanding of cyber-to-physical attack propagation	Integrated cyber–physical risk prediction and impact analysis	Digital twins, physics-informed AI, attack graphs
Communication security	Vulnerable IoT and edge communication infrastructures	Adaptive and resilient communication protection	AI-based IDS, zero trust, secure protocols
AI model security	Vulnerability to adversarial attacks and unreliable decisions	Trustworthy, explainable, and robust AI security	XAI, robust ML, secure FL, GenAI governance
Autonomous response	Limited automation and human dependency	Self-adaptive and self-healing defense mechanisms	Reinforcement learning, autonomous agents
Privacy preservation	Data sharing limitations across organizations	Secure collaborative intelligence	Federated learning, differential privacy
System resilience	Security mainly focused on prevention	Continuous operation under attack conditions	Resilience engineering, redundancy, adaptive control
Governance and human oversight	Lack of standards for autonomous cybersecurity	Responsible and certifiable autonomous security	AI governance, standards, human-AI collaboration

5. Conclusions

Autonomous CPS 2.0 represents a major advancement in the integration of physical processes with intelligent, distributed cyber capabilities. The incorporation of edge computing, AI/ML, GenAI, and FL enables unprecedented levels of adaptability, scalability, and real-time responsiveness across IoT ecosystems. However, these technological advancements also significantly expand the attack surface, introducing new security risks such as adversarial AI attacks, data manipulation, and model exploitation. As a result, traditional centralized security approaches are no longer sufficient, necessitating a shift toward proactive, decentralized, and intelligent security paradigms.

Key challenges related to privacy, interoperability, and accountability remain critical and require coordinated technical, organizational, and regulatory responses. Effective mitigation strategies must integrate zero-trust architectures, resilient system design, and continuous monitoring mechanisms to ensure operational stability and security. Real-world applications in domains such as industry, energy systems, and transportation highlight both the transformative potential of CPS 2.0 and the heightened exposure to cyber–physical threats. Achieving secure and trustworthy CPS 2.0 ecosystems will require a balanced approach that combines technological innovation, strong governance frameworks, and international collaboration to effectively address evolving cyber threats in IoT-driven environments.

Supplementary Materials: The following supporting information can be downloaded at: <https://www.mdpi.com/article/10.3390/electronics15153339/s1>, PRISMA 2020 Checklist (partial only) [15].

Author Contributions: Conceptualization, I.R., P.K. and D.M.; methodology, I.R., P.K. and D.M.; software, I.R. and D.M.; validation, I.R., P.K. and D.M.; formal analysis, I.R., P.K. and D.M.; investigation, I.R., P.K. and D.M.; resources, I.R., P.K. and D.M.; data curation, I.R. and D.M.; writing—original draft preparation, I.R., P.K. and D.M.; writing—review and editing, I.R., P.K. and D.M.; visualization, D.M.; supervision, I.R.; project administration, I.R.; funding acquisition, D.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research is being carried out as part of the project funded by the Polish Minister of Science and Higher Education under the ‘Regional Initiative of Excellence’ program (RID/SP/0048/2024/01) for Kazimierz Wielki University. The work presented in this paper has been financed under a grant to maintain the research potential of Kazimierz Wielki University.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial intelligence
API	Application Programming Interfaces
AR-PAO	Adaptive Reliability Planner-Attacker-Operator
CPPS	Cyber–physical power system
CPS	Cyber–Physical System
CNN	Convolutional neural network
DDoS	Distributed denial-of-service
DL	Deep learning
DLT	Distributed ledger technology
DOI	Digital Object Identifier
DP	Differential privacy
DSPN	Deterministic and stochastic Petri net
DT	Digital twin
EaCPS	Edge-assisted CPS
ECC	Elliptic curve cryptography
EEFED	Execution & Evaluation Dual Network Framework
FDIA	False data injection attacks
EIS	Edge Intelligence System
FL	Federated learning
FL-BIDPS	Federated learning and blockchain-integrated intrusion detection system
FL-CPS	Federated learning-enabled CPS
GenAI	Generative artificial intelligence
HCPS	Human–cyber–physical systems
HE	Homomorphic encryption
ICPS	Industrial CPS
IDS	Intrusion Detection System
IID	Independent and identically distributed
IoT	Internet of Things
IoUT	Internet of Underwater Things
ITS	Intelligent Transportation System
LSTM	Long short-term memory network
M2M	Machine-to-machine
MEC	Mobile edge computing

MITM	Man-in-the-middle
ML	Machine learning
PEF-CAPD	Privacy-Enhanced Federated Cyber Physical and Attack Detection
PET	Privacy-enhancing technology
PLC	Programmable Logic Controllers
RQ	Research question
SCADA	Supervisory Control and Data Acquisition
SDN	Software-defined network
SDG	Sustainable Development Goal
SVM	Support vector machine
VCPS	Vehicular Cyber-Physical System
XAI	eXplainable AI

References

1. Czczot, G.; Rojek, I.; Mikołajewski, D.; Sangho, B. AI in IIoT Management of Cybersecurity for Industry 4.0 and Industry 5.0 Purposes. *Electronics* **2023**, *12*, 3800. [\[CrossRef\]](#)
2. Adil, M.; Farouk, A.; Abulkasim, H.; Ali, A.; Song, H.; Jin, Z. NG-ICPS: Next Generation Industrial-CPS, Security Threats in the Era of Artificial Intelligence, and Open Challenges with Future Research Directions. *IEEE Internet Things J.* **2025**, *12*, 1343–1367. [\[CrossRef\]](#)
3. Zhang, L.; Yu, H.; Wang, C.; Hu, Y.; He, W.; Yu, D. A digital solution for CPS-based machining path optimization for CNC systems. *J. Intell. Manuf.* **2025**, *36*, 1261–1290.
4. Czczot, G.; Rojek, I.; Mikołajewski, D. Analysis of Cyber Security Aspects of Data Transmission in Large-Scale Networks Based on the LoRaWAN Protocol Intended for Monitoring Critical Infrastructure Sensors. *Electronics* **2023**, *12*, 2503. [\[CrossRef\]](#)
5. Yu, Z.; Gao, H.; Cong, X.; Wu, N.; Song, H.H. A Survey on Cyber-Physical Systems Security. *IEEE Internet Things J.* **2023**, *10*, 21670–21686. [\[CrossRef\]](#)
6. Lu, Y.; Wang, D.; Obaidat, M.S.; Vijayakumar, P. Edge-Assisted Intelligent Device Authentication in Cyber-Physical Systems. *IEEE Internet Things J.* **2023**, *10*, 3057–3070. [\[CrossRef\]](#)
7. Oks, S.J.; Jalowski, M.; Lechner, M.; Mirschberger, S.; Merklein, M.; Vogel-Heuser, B.; Möslin, K.M. Cyber-Physical Systems in the Context of Industry 4.0: A Review, Categorization, and Outlook. *Inf. Syst. Front.* **2022**, *26*, 1731–1772. [\[CrossRef\]](#)
8. Fu, R.; Chen, J.; Lin, Y.; Zou, A.; Chen, C.; Guan, X.; Ma, Y. Smart Sensing and Communication Co-Design for IIoT-Based Control Systems. *IEEE Internet Things J.* **2024**, *11*, 3994–4014. [\[CrossRef\]](#)
9. Hosen, A.S.M.S.; Sharma, P.K.; Ra, I.-H.; Cho, G.H. SPTM-EC: A Security and Privacy-Preserving Task Management in Edge Computing for IIoT. *IEEE Trans. Ind. Inform.* **2022**, *18*, 6330–6339. [\[CrossRef\]](#)
10. Mohammed, G.B.; Selvarajan, S.; Ravi, A.K.; Sangeetha, K.; Khadidos, A.O.; Vatchala, S. An Analytical Framework for the Industrial Internet of Things (IIoT): Importance, Recent Challenges, and Enabling Technologies. In *Industry Automation: The Technologies, Platforms and Use Cases*; River Publishers: Nordjylland, Denmark, 2024.
11. Sánchez-Zumba, A.; Avila-Pesantez, D. Cybersecurity for Industrial IoT: Threats, Vulnerabilities, and Solutions: A Brief Review. In *Proceedings of the Eighth International Congress on Information and Communication Technology (ICICT 2023), London, UK, 20–23 February 2023*; Yang, X.S., Sherratt, R.S., Dey, N., Joshi, A., Eds.; Lecture Notes in Networks and Systems; Springer: Singapore, 2023; Volume 693.
12. Chalapathi, G.S.S.; Chamola, V.; Vaish, A.; Buyya, R. Industrial Internet of Things (IIoT) Applications of Edge and Fog Computing: A Review and Future Directions. In *Fog/Edge Computing for Security, Privacy, and Applications*; Chang, W., Wu, J., Eds.; Advances in Information Security; Springer: Cham, Switzerland, 2021; Volume 83.
13. Tang, S.; Chen, L.; He, K.; Xia, J.; Fan, L.; Nallanathan, A. Computational Intelligence and Deep Learning for Next-Generation Edge-Enabled Industrial IoT. *IEEE Trans. Netw. Sci. Eng.* **2023**, *10*, 2881–2893. [\[CrossRef\]](#)
14. Hasan, B.T.; Idrees, A.K. Edge Computing for IoT. In *Learning Techniques for the Internet of Things*; Springer Nature: Cham, Switzerland, 2023; pp. 1–20.
15. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ* **2021**, *372*, n71. [\[CrossRef\]](#) [\[PubMed\]](#)
16. Li, L.; Yang, R.; Shu, Z.; Wu, L. Event-Based Secure State Estimation for 2-D CPSs Under Deception Attacks: A Game Theoretic Approach. *IEEE Trans. Ind. Inform.* **2025**, *21*, 1017–1025. [\[CrossRef\]](#)
17. Bi, Y.; Peng, F.; Sun, K.; Wang, T.; Qiu, J. Fixed-Time Adaptive Sliding-Mode Resilient Control for Strict-Feedback Nonlinear CPSs Against Deception Attacks. *IEEE Trans. Syst. Man. Cybern. Syst.* **2025**, *55*, 843–851. [\[CrossRef\]](#)

18. Garcia, L.; Mirkovic, J.; Balenson, D.M.; Kline, E.; Pradkin, Y.; Choffnes, D.R.; Dubois, D.J.; Benzel, T.; Ravi, S.; Barnes, J.; et al. SPHERE CPS Enclave: A Reconfigurable Testbed for Industrial Control System Security Experimentation. In *Proceedings of the ICCPS '25: ACM/IEEE 16th International Conference on Cyber-Physical Systems, Irvine, CA, USA, 6–9 May 2025*; Association for Computing Machinery: New York, NY, USA, 2025; p. 46. [\[CrossRef\]](#)
19. Zhan, N.; Su, H.; Yang, M.; Gu, B. Reset controller synthesis: A correct-by-construction way to the design of CPS. *Res. Dir. Cyber Phys. Syst.* **2024**, *2*, e7. [\[CrossRef\]](#)
20. Rojek, I.; Kotlarz, P.; Dorożyński, J.; Mikołajewski, D. Sixth-Generation (6G) Networks for Improved Machine-to-Machine (M2M) Communication in Industry 4.0. *Electronics* **2024**, *13*, 1832. [\[CrossRef\]](#)
21. Bapatla, A.K.; Mohanty, S.P.; Kougianos, E. FortiRx 2.0: Smart Privacy-Preserved Demand Forecasting of Prescription Drugs in Healthcare-CPS. In *Proceedings of the 2023 OITS International Conference on Information Technology (OCIT), Raipur, India, 13–15 December 2023*; IEEE: New York, NY, USA, 2023; pp. 438–443.
22. Mei, Q.; Xiong, H.; Chen, C.M. Blockchain-Enabled Privacy-Preserving Authentication Mechanism for Transportation CPS with Cloud-Edge Computing. *IEEE Trans. Eng. Manag.* **2024**, *71*, 12463–12474. [\[CrossRef\]](#)
23. Arif, T.; Jo, B.; Park, J. H Blockchain-Enabled IDPS and Federated Learning for Enhancing CPS Security against Advanced Persistent Threats in Zero Trust Architectures. *Hum.-Centric Comput. Inf. Sci.* **2025**, *15*, 022.
24. Consul, P.; Budhiraja, I.; Kumar, N. Security Reassessing in UAV-Assisted Cyber-Physical Systems based on Federated Learning. In *Proceedings of the 2022 IEEE Military Communications Conference (MILCOM), Rockville, MD, USA, 28 November–2 December 2022*.
25. Basak, S.; Chatterjee, K.; Singh, A. DPPT: A differential privacy preservation technique for cyber-physical system. *Comput. Electr. Eng.* **2023**, *109*, 108661. [\[CrossRef\]](#)
26. Zhukabayeva, T.; Zholshiyeva, L.; Karabayev, N.; Khan, S.; Alnazzawi, N. Cybersecurity Solutions for Industrial Internet of Things–Edge Computing Integration: Challenges, Threats, and Future Directions. *Sensors* **2025**, *25*, 213. [\[CrossRef\]](#) [\[PubMed\]](#)
27. Raghunath, K.M.K.; Mahesh, T.R.; Almusharraf, A. Diffusion-Driven Proxy Learning Strategy with Secure Peer Interactions for Generative Intelligence in Cyber-Physical System. *JOVE-J. Vis. Exp.* **2025**, 220.
28. Lian, Y.D.; Yang, Q.F.; Zhang, L.W. Cyber-Physical System-Based Heuristic Planning and Scheduling Method for Multiple Automatic Guided Vehicles in Logistics Systems. *IEEE Trans. Ind. Inform.* **2021**, *17*, 7882–7893. [\[CrossRef\]](#)
29. Gaba, S.; Buddhiraja, I.; Makkar, A. Federated Learning Based Secured Computational Offloading in Cyber-Physical IoST Systems. In *Proceedings of the 5th International Conference on Recent Trends in Image Processing and Pattern Recognition (RTIP2R 2022), Kingsville, TX, USA, 1–2 December 2022*; pp. 344–355.
30. Seid, A.M.; Abishu, H.N.; Guizani, M. HDFRL-empowered Energy Efficient Resource Allocation for Aerial MEC-enabled Smart City Cyber Physical System in 6G. In *Proceedings of the 19th IEEE International Wireless Communications and Mobile Computing (IEEE IWCMC), Marrakesh, Morocco, 19–23 June, 2023*; pp. 836–841.
31. Thanganadar, H.; Yaseen, S.M.; Vijayakumar, P. 6G Wireless Communication Cyber Physical System Based Smart Healthcare Using Quantum Optimization with Machine Learning. *Wirel. Pers. Commun.* **2024**. [\[CrossRef\]](#)
32. Zheng, S.W.; Hu, J.; Li, K. Meta Representation-Based Personalized Federated Continual Learning in Edge Computing Systems. *IEEE Trans. Comput. Soc. Syst.* **2025**, 1–12. [\[CrossRef\]](#)
33. Li, Y.; Wei, X.H.; Shahidepour, M. Detection of False Data Injection Attacks in Smart Grid: A Secure Federated Deep Learning Approach. *IEEE Trans. Smart Grid* **2022**, *13*, 4862–4872. [\[CrossRef\]](#)
34. Xu, Z.Y.; Zhang, Y.Q.; Qi, Q. Dynamic resource provisioning for cyber-physical systems in cloud-fog-edge computing. *J. Cloud Comput.-Adv. Syst. Appl.* **2020**, *9*, 1. [\[CrossRef\]](#)
35. Dong, Y.Y.; Dai, F.; Qin, M.M. A Privacy-Preserving Deep Learning Scheme for Edge-enhanced Smart Homes. In *Proceedings of the IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Calabria, Italy, 12–15 September 2022*; pp. 487–492.
36. Matsuzaki, K.; Sawada, K.; Honiden, S. Remote Security Assessment for Cyber-Physical Systems: Adapting Design Patterns for Enhanced Diagnosis. In *Proceedings of the 20th International Conference on Security and Cryptography (SECRYPT), Rome, Italy, 10–12 July 2023*; pp. 805–812.
37. Rajagopal, M.P.; Natesan, G. PEF-CAPD: A Privacy Enhanced Federated Cyber Physical and Attack Detection Framework for Edge-Cloud-Blockchain Enabled Smart Healthcare Environment. *Trans. Emerg. Telecommun. Technol.* **2025**, *36*, 7. [\[CrossRef\]](#)
38. Quan, M.K.; Pathirana, P.N.; Poor, H.V. Federated Learning for Cyber Physical Systems: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2026**, *28*, 3751–3790. [\[CrossRef\]](#)
39. Kim, S.; Cho, W. Accelerating Homomorphic Comparison Operations for Thresholding Using an Asymmetric Input Range and Input Scaling. In *Proceedings of the 34th Great Lakes Symposium on VLSI (GLSVLSI), Clearwater, FL, USA, 12–14 June 2024*; pp. 427–432.

40. Singh, R.K.B.; Reddy, K.H.K. Edge-AI empowered Cyber-Physical Systems: A comprehensive review on performance analysis. *Comput. Sci. Rev.* **2025**, *58*, 100769. [\[CrossRef\]](#)
41. Popli, M.S.; Singh, R.P.; Mamun, M. A Federated Learning Framework for Enhanced Data Security and Cyber Intrusion Detection in Distributed Network of Underwater Drones. *IEEE Access* **2015**, *13*, 12634–12646.
42. Alnaim, A.K.; Alwakeel, A.M. Zero Trust Strategies for Cyber-Physical Systems in 6G Networks. *Mathematics* **2025**, *13*, 1108. [\[CrossRef\]](#)
43. He, Y.P.; Yan, T.J.; Xia, Y.Q. MCFL: A federated learning framework for network traffic classification in dynamic networks. *Future Gener. Comput. Syst.* **2026**, *181*, 108434. [\[CrossRef\]](#)
44. Firdaus, M.; Rhee, K.H. A Joint Framework to Privacy-Preserving Edge Intelligence in Vehicular Networks. In Proceedings of the 23rd World Conference on Information Security Applications, Jeju Island, Republic of Korea, 24–26 August 2022; pp. 156–167.
45. Wang, H.Y.; Fan, K.; Yang, Y.T. Secure and Efficient Data-Privacy-Preserving Scheme for Mobile Cyber-Physical Systems. *IEEE Internet Things J.* **2022**, *9*, 22375–22388. [\[CrossRef\]](#)
46. Huang, X.T.; Liu, J.; Lyu, H. EEFED: Personalized Federated Learning of Execution&Evaluation Dual Network for CPS Intrusion Detection. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 41–56. [\[CrossRef\]](#)
47. Soomro, I.A.; Khan, H.U.R.; Alotaibi, N.N. Lightweight Privacy-Preserving Federated Deep Intrusion Detection for Industrial Cyber-Physical System. *J. Commun. Netw.* **2024**, *26*, 632–649. [\[CrossRef\]](#)
48. Andrade, E.; Machida, F. Analysis of Software Aging Impacts on Plant Anomaly Detection with Edge Computing. In Proceedings of the 30th IEEE International Symposium on Software Reliability Engineering (ISSRE), Berlin, Germany, 28–31 October 2019; pp. 204–210.
49. Chan, M.; Garcia, L.; Srivastava, M. Leaking Through the Physics: Covert Cyber-Physical Data Exfiltration Through Unobserved Physics. In Proceedings of the 2nd International Conference on Security and Privacy in Cyber-Physical Systems and Smart Vehicles-SmartSP, Salt Lake City, UT, USA, 1–2 December 2025; Volume 622, pp. 3–25.
50. Lu, Z.H. Application of Deep Learning Video Signal Processing Technology in University Management. *J. Inf. Sci. Eng.* **2025**, *41*, 1217–1238.
51. Olowononi, F.O.; Rawat, D.B.; Liu, C.M. Federated Learning with Differential Privacy for Resilient Vehicular Cyber Physical Systems. In Proceedings of the IEEE 18th Annual Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2021.
52. Wang, X.; Chen, Y.Z.; Dobre, O.A. Federated Learning for Anomaly Detection: A Case of Real-World Energy Storage Deployment. In Proceedings of the IEEE International Conference on Communications (ICC), Seoul, Republic of Korea, 16–20 May 2022; pp. 4312–4317.
53. Firdaus, M.; Larasati, H.T.; Rhee, K.H. A Blockchain-Assisted Distributed Edge Intelligence for Privacy-Preserving Vehicular Networks. *CMC-Comput. Mater. Contin.* **2023**, *76*, 2959–2978. [\[CrossRef\]](#)
54. Rehman, U.U. A systematic literature review on data privacy and security techniques in smart cities: Trends, gaps, and future directions. *Computing* **2025**, *107*, 10. [\[CrossRef\]](#)
55. Zhang, Y.; Ma, L.; Yang, C.; Wang, G.; Dai, W. Asynchronous Event-Triggered Control for Two-Time-Scale CPSs with Dual-Scale Channel: Dealing with Hybrid Attacks. *IEEE Trans. Control. Netw. Syst.* **2023**, *11*, 999–1011.
56. Chen, W.D.; Li, Y.X.; Liu, L.; Zhao, X.D.; Niu, B.; Han, L.M. Nussbaum-Based Adaptive Fault-Tolerant Control for Nonlinear CPSs with Deception Attacks: A New Coordinate Transformation Technology. *IEEE Trans. Cybern.* **2024**, *54*, 1212–1222. [\[CrossRef\]](#) [\[PubMed\]](#)
57. Ju, Y.; Yang, M.; Chakraborty, C.; Liu, L.; Pei, Q.; Xiao, M.; Yu, K. Reliability-Security 1 Tradeoff Analysis in mmWave Ad Hoc-based CPS. *ACM Trans. Sens. Netw.* **2024**, *20*, 28. [\[CrossRef\]](#)
58. Liu, J.; Tang, Y.; Zhao, H.; Wang, X.; Li, F.; Zhang, J. CPS Attack Detection under Limited Local Information in Cyber Security: An Ensemble Multi-Node Multi-Class Classification Approach. *ACM Trans. Sens. Netw.* **2024**, *20*, 33. [\[CrossRef\]](#)
59. D'Mello, S.K.; Duran, N.D.; Michaels, A.; Stewart, A.E.B. Improving collaborative problem-solving skills via automated feedback and scaffolding: A quasi-experimental study with CPSCoach 2.0. *User Model. User Adapt. Interact.* **2024**, *34*, 1087–1125. [\[CrossRef\]](#)
60. Gaur, V.; Verma, R. Revolutionizing industries through cyber-physical systems: A systematic review. *Discov. Comput.* **2026**, *29*, 250. [\[CrossRef\]](#)
61. Alquahtani, H.; Ahuja, P. Secure autonomous cyber defense with LLM agents: A systematic review of autonomy, tool-augmented reasoning, and governance constraints. *Comput. Electr. Eng.* **2026**, *125*, 111184. [\[CrossRef\]](#)
62. Angrisani, L.; D'Arco, M.; D'Iorio, M.; Lo Regio, F. Quantum-secured distributed measurement systems for critical infrastructures operations. *Measurement* **2026**, *278*, 121738. [\[CrossRef\]](#)
63. Hynek, N.; Gavurova, B.; Kubak, M.; Senk, M. Expert views on integrating robots, drones, cameras, and AI into critical infrastructure protection and national security: An opportunity for sustainable entrepreneurship. *Int. Entrep. Manag.* **2025**, *22*, 37. [\[CrossRef\]](#)
64. Gopal, T.V. Cyber-Physical Systems for Industry 4.0 and Beyond. *Smart Innov. Syst. Technol.* **2026**, *119*, 319–332. [\[CrossRef\]](#)

65. Peng, H.; Kan, Z.; Liu, C.; Baker, T.; Zhao, D. Risk Assessment of CPS Composed of Edge Consumer Electronics Under Intentional Attack. *IEEE Consum. Electron. Mag.* **2022**, *11*, 36–41. [\[CrossRef\]](#)
66. Singhal, C.; Rajesh, A. Heuristic trust-based neighbour centric routing for CPS-enabled wireless sensor and ad hoc network. *Int. J. Inf. Comput. Secur.* **2021**, *16*, 120–136. [\[CrossRef\]](#)
67. Harbin, J.; Burns, A.; Davis, R.I.; Soares Indrusiak, L.; Bate, I.; Griffin, D. The AirTight Protocol for Mixed Criticality Wireless CPS. *ACM Trans. Cyber Phys. Syst.* **2020**, *4*, 1–28.
68. Saxena, N.; Cárdenas, A.A.; Beyah, R.; Lu, R.; Choo, K.K.R.; Chen, Y. Introduction to the Special Issue on User-Centric Security and Safety for CPS. *ACM Trans. Cyber Phys. Syst.* **2020**, *4*, 29. [\[CrossRef\]](#)
69. Enoch, O.S.; Umoga, U.J.; Obaigbena, A.; Jacks, B.S.; Ugwuanyi, D.E.; Daraojimba, A.I.; Lottu, O.A. Current State and Prospectsof Edge Computing within the Internet of Things (IoT) Ecosystem. *Int. J. Sci. Res. Arch.* **2024**, *11*, 1863–1873. [\[CrossRef\]](#)
70. Karyemsetty, N.; Narasimha, P.B.; Tejaswi, M.P.; Sivaji, V.N.; Kamal, C.L.V.; Samatha, B. Cybersecurity Fortification in Edge Computing through the Synergy of Deep Learning. In Proceedings of the 2023 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), Kirtipur, Nepal, 11–13 October 2023; pp. 1154–1160.
71. Al-Doghman, F.; Moustafa, N.; Khalil, I.; Sohrabi, N.; Tari, Z.; Zomaya, A.Y. AI-Enabled Secure Microservices in Edge Computing: Opportunities and Challenges. *IEEE Trans. Serv. Comput.* **2023**, *16*, 1485–1504. [\[CrossRef\]](#)
72. Fomichev, D.S. Intelligent Communication for Internet of Things (IoRT). In Proceedings of the International Conference on Recent Innovations in Computing (ICRIC 2022), Samba, India, 13–14 May 2022.
73. Abosata, N.; Al-Rubaye, S.; Inalhan, G.; Emmanouilidis, C. Internet of Things for System Integrity: A Comprehensive Survey on Security, Attacks and Countermeasures for Industrial Applications. *Sensors* **2021**, *21*, 3654. [\[CrossRef\]](#) [\[PubMed\]](#)
74. Sun, D.; Hu, J.; Wu, H.; Wu, J.; Yang, J.; Sheng, Q.; Dustdar, S. A Comprehensive Survey on Collaborative Data-Access Enablers in the IIoT. *ACM Comput. Surv.* **2023**, *56*, 1–37. [\[CrossRef\]](#)
75. Lee, E.; Seo, Y.D.; Oh, S.-R.; Kim, Y.G. A Survey on Standards for Interoperability and Security in the Internet of Things. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 1020–1047. [\[CrossRef\]](#)
76. Luxmi, D.; Armstrong, E.; Newe, T. Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap. *Sensors* **2021**, *21*, 3901. [\[CrossRef\]](#)
77. Behnke, I.; Austad, H. Real-Time Performance of Industrial IoT Communication Technologies: A Review. *IEEE Internet Things J.* **2023**, *11*, 7399–7410. [\[CrossRef\]](#)
78. Khan, F.; Jan, M.A.; Rehman, A.U.; Mastorakis, S.; Alazab, M.; Watters, P. A Secured and Intelligent Communication Scheme for IIoT-enabled Pervasive Edge Computing. *IEEE Trans. Ind. Inform.* **2021**, *17*, 5128–5137. [\[CrossRef\]](#)
79. Wang, P.; Yang, L.T.; Qian, G.; Li, J.; Yan, Z. HO-OTSVD: A Novel Tensor Decomposition and Its Incremental Decomposition for Cyber-Physical-Social Networks (CPSN). *IEEE Trans. Netw. Sci. Eng.* **2020**, *7*, 713–725. [\[CrossRef\]](#)
80. Alzahrani, A.; Asghar, M.Z. Cyber vulnerabilities detection system in logistics-based IoT data exchange. *Egypt. Inform. J.* **2024**, *25*, 100448. [\[CrossRef\]](#)
81. Rathee, G.; Ahmad, F.; Sandhu, R.; Kerrache, C.A.; Azad, M.A. On the design and implementation of a secure blockchain-based hybrid framework for Industrial Internet-of-Things. *Inf. Process. Manag.* **2021**, *58*, 102526. [\[CrossRef\]](#)
82. Nawaz, A.; Queralta, J.P.; Guan, J.; Awais, M.; Gia, T.N.; Bashir, A.K.; Kan, H.; Westerlund, T. Edge Computing to Secure IoT Data Ownership and Trade with the Ethereum Blockchain. *Sensors* **2020**, *20*, 3965. [\[CrossRef\]](#) [\[PubMed\]](#)
83. Zainudin, A.; Putra, M.A.P.; Alief, R.N.; Kim, D.-S.; Lee, J.-M. Blockchain-aided Collaborative Threat Detection for Securing Digital Twin-based IIoT Networks. In Proceedings of the ICC 2024—IEEE International Conference on Communications, Denver, CO, USA, 9–13 June 2024; pp. 4656–4661.
84. Okfie, M.I.H.; Mishra, S. Anomaly Detection in IIoT Transactions using Machine Learning: A Lightweight Blockchain-based Approach. *Eng. Technol. Appl. Sci. Res.* **2024**, *14*, 14645–14653. [\[CrossRef\]](#)
85. Shan, A.; Myeong, S. Proactive Threat Hunting in Critical Infrastructure Protection through Hybrid Machine Learning Algorithm Application. *Sensors* **2024**, *24*, 4888. [\[CrossRef\]](#) [\[PubMed\]](#)
86. Pinto, A.; Herrera, L.-C.; Donoso, Y.; Gutierrez, J.A. Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure. *Sensors* **2023**, *23*, 2415. [\[CrossRef\]](#) [\[PubMed\]](#)
87. Hazra, A.; Alkhayyat, A.; Adhikari, M. Blockchain for cybersecurity in edge networks. *IEEE Consum. Electron. Mag.* **2022**, *13*, 97–102. [\[CrossRef\]](#)
88. Zhang, T.; Xue, C.; Wang, J.; Yun, Z.; Lin, N.; Han, S. A Survey on Industrial Internet of Things (IIoT), Testbeds for Connectivity Research. *arXiv* **2024**, arXiv:2404.17485v2.
89. Mehedi, S.T.; Anwar, A.; Rahman, Z.; Ahmed, K.; Islam, R. Dependable Intrusion Detection System for IoT: A Deep Transfer. Learning Based Approach. *IEEE Trans. Ind. Inform.* **2023**, *19*, 1006–1017. [\[CrossRef\]](#)
90. Jamalipour, A.; Murali, S. A Taxonomy of Machine-Learning-Based Intrusion Detection Systems for the Internet of Things: A Survey. *IEEE Internet Things J.* **2022**, *9*, 9444–9466. [\[CrossRef\]](#)

91. Alsaleh, S.S.; El Bachir Menai, M.; Al-Ahmadi, S. Federated Learning-Based Model to Lightweight IDSs for Heterogeneous IoT Networks: State-of-the-Art, Challenges, and Future Directions. *IEEE Access* **2024**, *12*, 134256–134272. [\[CrossRef\]](#)
92. Zohourian, A.; Dadkhah, S.; Molyneaux, H.; Neto, E.C.P.; Ghorbani, A.A. IoT-PRIDS: Leveraging packet representations for intrusion detection in IoT networks. *Comput. Secur.* **2024**, *146*, 104034. [\[CrossRef\]](#)
93. Liu, D.; Ding, Y.; Yu, G.; Zhong, Z.; Song, Y. Privacy-preserving dynamic auditing for regenerating code-based storage in cloud-fog-assisted IIoT. *Internet Things* **2024**, *25*, 101084. [\[CrossRef\]](#)
94. Consul, P.; Budhiraja, I.; Garg, D.; Garg, S.; Kaddoum, G.; Hassan, M.M. SFL-TUM: Energy efficient SFRL method for large scale AI model's task offloading in UAV-assisted MEC networks. *Veh. Commun.* **2024**, *48*, 100790. [\[CrossRef\]](#)
95. Li, K.; Wang, H.; Zhou, M.; Zhu, H.; Sun, L. Cascading Threat Analysis of IoT Devices in Trigger-Action Platforms. *IEEE Internet Things J.* **2024**, *11*, 12240–12251. [\[CrossRef\]](#)
96. Zainudin, A.; Ahakonye, L.A.C.; Akter, R.; Kim, D.-S.; Lee, J.-M. An Efficient Hybrid-DNN for DDoS Detection and Classification in Software-Defined IIoT Networks. *IEEE Internet Things J.* **2023**, *10*, 8491–8504. [\[CrossRef\]](#)
97. Houda, Z.A.E.; Brik, B.; Ksentini, A.; Khoukhi, L.; Guizani, M. When Federated Learning Meets Game Theory: A Cooperative Framework to Secure IIoT Applications on Edge Computing. *IEEE Trans. Ind. Inform.* **2022**, *18*, 7988–7997. [\[CrossRef\]](#)
98. Niu, S.; Shao, H.; Su, Y.; Wang, C. Efficient heterogeneous signcryption scheme based on Edge Computing for Industrial Internet of Things. *J. Syst. Archit.* **2023**, *136*, 102836. [\[CrossRef\]](#)
99. Bayar, A.; Sener, U.; Kayabay, K.; Eren, P.E. Edge computing applications in industrial IoT: A literature review. In Proceedings of the International Conference on the Economics of Grids, Clouds, Systems, and Service, Izola, Slovenia, 13–15 September 2022; Springer Nature: Cham, Switzerland, 2022; pp. 124–131.
100. Sun, J.; Yang, Z. ObjSim: Efficient testing of cyber-physical systems. In *Proceedings of the ISSTA '20: 29th ACM SIGSOFT International Symposium on Software Testing and Analysis, Virtual, 19 July 2020*; Association for Computing Machinery: New York, NY, USA, 2020; pp. 1–2.
101. Zhang, J.; Zhu, Y.; Xiao, F. Modelling and analysis of real-time and reliability for WSN-based CPS. *Int. J. Internet Protoc. Technol.* **2019**, *12*, 76–84. [\[CrossRef\]](#)
102. Kong, X.; Lu, Z.; Guo, X.; Zhang, J.; Li, H. Resilience Evaluation of Cyber-Physical Power System Considering Cyber Attacks. *IEEE Trans. Reliab.* **2024**, *73*, 245–256. [\[CrossRef\]](#)
103. Du, M.; Zhang, X.; Guerrero, J.M. Adaptive Robust Planner-Attacker-Operator Model Against Multistage Uncertain Malicious Attacks for Power Systems with Volatile Wind Power. *IEEE Trans. Ind. Inform.* **2026**, *22*, 5378–5389. [\[CrossRef\]](#)
104. Tan, F.; Liu, L.; Winter, S.; Wang, Q.; Suri, N.; Bu, L.; Peng, Y.; Liu, X.; Peng, X. Cross-Domain Noise Impact Evaluation for Black Box Two-Level Control CPS. *ACM Trans. Cyber Phys. Syst.* **2019**, *3*, 2.
105. Carreras, M.; Deriu, G.; Meloni, P. Flexible Acceleration of Convolutions on FPGAs: NEURAghe 2.0. In Proceedings of the CPS Summer School, PhD Workshop, Alghero, Italy, 22–28 September 2019; pp. 60–71.
106. Zheng, Z.; Mao, W.; Wu, F.; Chen, G. Challenges and Opportunities in IoT Data Markets. In *Proceedings of the CPS-IoT Week '19: Cyber-Physical Systems and Internet of Things Week 2019, Montreal, QC, Canada, 15 April 2019*; Association for Computing Machinery: New York, NY, USA, 2019; pp. 1–2.
107. Wang, F.Y.; Yuan, Y.; Rong, C.; Zhang, J.J. Parallel Blockchain: An Architecture for CPSS-Based Smart Societies. *IEEE Trans. Comput. Soc. Syst.* **2018**, *5*, 303–310. [\[CrossRef\]](#)
108. Yang, W.; Xu, C.; Pan, M.; Ma, X.; Lu, J. Improving Verification Accuracy of CPS by Modeling and Calibrating Interaction Uncertainty. *ACM Trans. Internet Techn.* **2018**, *18*, 20. [\[CrossRef\]](#)
109. Böhm, W.; Stierand, I.; Vogelsang, A.; Weyer, T. 4th International Workshop on Emerging Ideas and Trends in Engineering of Cyber-Physical Systems (EITEC'18). In Proceedings of the 2018 4th International Workshop on Emerging Ideas and Trends in the Engineering of Cyber-Physical Systems (EITEC), Porto, Portugal, 10–11 April 2018; pp. 1–2.
110. Yang, G.; Zhou, X. Intelligent CPS: Features and challenges. *Sci. China Inf. Sci.* **2016**, *59*, 050102. [\[CrossRef\]](#)
111. Parveen Sultana, H.; Venkata Krishna, P. Priority focused medium access control in wireless sensor actuator networks for CPS. *Int. J. Commun. Netw. Distrib. Syst.* **2016**, *16*, 99–113. [\[CrossRef\]](#)
112. Krzysztoń, E.; Rojek, I.; Mikołajewski, D. A Comparative Analysis of Anomaly Detection Methods in IoT Networks: An Experimental Study. *Appl. Sci.* **2024**, *14*, 11545. [\[CrossRef\]](#)
113. Ellappan, V.; Mahendran, A.; Subramanian, M.; Jotheeswaran, J.; Khadidos, A.O.; Khadidos, A.O.; Selvarajan, S. Sliding principal component and dynamic reward reinforcement learning based IIoT attack detection. *Sci. Rep.* **2023**, *13*, 20843. [\[CrossRef\]](#) [\[PubMed\]](#)
114. Tian, Y.; Li, T.; Xiong, J.; Bhuiyan, M.Z.A.; Ma, J.; Peng, C. A blockchain-based machine learning framework for edge services in IIoT. *IEEE Trans. Ind. Inform.* **2021**, *18*, 1918–1929. [\[CrossRef\]](#)
115. Jiang, D.; Wang, Z.; Wang, Y.; Tan, L.; Wang, J.; Zhang, P. A Blockchain-Reinforced Federated Intrusion Detection Architecture for IIoT. *IEEE Internet Things J.* **2024**, *11*, 26793–26805. [\[CrossRef\]](#)

116. Wang, W.; Xu, H.; Alazab, M.; Gadekallu, T.R.; Han, Z.; Su, C. Blockchain-Based Reliable and Efficient Certificateless Signature for IIoT Devices. *IEEE Trans. Ind. Inform.* **2022**, *18*, 7059–7067. [\[CrossRef\]](#)
117. Abou El Houda, Z.; Brik, B.; Ksentini, A. Securing IIoT applications in 6G and beyond using adaptive ensemble learning and zero-touch multi-resource provisioning. *Comput. Commun.* **2024**, *216*, 260–273. [\[CrossRef\]](#)
118. Aouedi, O.; Piamrat, K. Toward a Scalable and Energy-Efficient Framework for Industrial Cloud-Edge-IoT Continuum. *IEEE Internet Things Mag.* **2024**, *7*, 14–20. [\[CrossRef\]](#)
119. Hassini, K.; Khalis, S.; Habibi, O.; Chemmakha, M.; Lazaar, M. An end-to-end learning approach for enhancing intrusion detection in Industrial-Internet of Things. *Knowl. Based Syst.* **2024**, *294*, 111785. [\[CrossRef\]](#)
120. Nandanwar, H.; Katarya, R. Deep learning enabled intrusion detection system for Industrial IOT environment. *Expert Syst. Appl.* **2024**, *249*, 123808. [\[CrossRef\]](#)
121. Kayan, H.; Nunes, M.; Rana, O.; Burnap, P.; Perera, C. Cybersecurity of industrial cyber-physical systems: A review. *ACM Comput. Surv.* **2022**, *54*, 1–35. [\[CrossRef\]](#)
122. Ahmed, S.F.; Bin Alam, S.; Hoque, M.; Lameesa, A.; Afrin, S.; Farah, T.; Kabir, M.; Shafiullah, G.; Muyeen, S. Industrial Internet of Things enabled technologies, challenges, and future directions. *Comput. Electr. Eng.* **2023**, *110*, 108847. [\[CrossRef\]](#)
123. Sharma, M.; Elmiligi, H.; Gebali, F. Network Security and Privacy Evaluation Scheme for Cyber Physical Systems (CPS). In *Handbook of Big Data Privacy*; Springer International Publishing: Cham, Switzerland, 2020; pp. 191–217. [\[CrossRef\]](#)
124. Termanini, A.; Bourdoucen, H.; Al-Abri, D.; Al Maashri, A. Intrusion Detection Datasets for IIoT and ICS: A Taxonomic Review with a Decision-Aid Scoring Rubric. *Sensors* **2026**, *26*, 4099. [\[CrossRef\]](#) [\[PubMed\]](#)
125. Marcheschi, P.; Pisani, M.; Dalmiani, S. From Simulation to Healthcare: KINAITICS' AI Framework for Cyber-Physical Security. *Open Res. Eur.* **2026**, *6*, 170. [\[CrossRef\]](#) [\[PubMed\]](#)
126. Salam, A.; Shakir, A.T.; Javaid, Q.; Masini, B.M.; Ahmad, M.; Wahid, I. Secure IIoT architecture with blockchain-enabled anomaly detection for water distribution cyber-physical systems. *Sci. Rep.* **2026**. [\[CrossRef\]](#) [\[PubMed\]](#)
127. Wang, Z.; Chen, J.; Wei, Z.; Lin, L.; Tong, G. SafeCodeRL: Security-Constrained Multi-Agent Reinforcement Learning for Trustworthy LLM-Generated IoT/CPS Software. *Sensors* **2026**, *26*, 3502. [\[CrossRef\]](#) [\[PubMed\]](#)
128. Kazemi, H.; Khorasani, K. Secure Distributed State Estimation in Nonlinear Cyber-Physical Systems Using Sensor Networks. *IEEE Trans. Cybern.* **2026**. [\[CrossRef\]](#) [\[PubMed\]](#)
129. Ray, I.; Thomas, R.K.; Cárdenas, A.A. Assurance Techniques for Industrial Control Systems (ICS). In Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or Privacy, CPS-SPC 2015, Denver, CO, USA, 16 October 2015.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.