electronics

MDPI

Review

A Review on Federated Learning Architectures for Privacy-Preserving AI: Lightweight and Secure Cloud–Edge–End Collaboration

Shanhao Zhan [1], Lianfen Huang [1,2], Gaoyu Luo [1], Shaolong Zheng [1], Zhibin Gao [3,*] and Han-Chieh Chao [4,5,6,*]

[1] School of Informatics, Xiamen University, Xiamen 361005, China; shanhao@stu.xmu.edu.cn (S.Z.); lfhuang@xmu.edu.cn (L.H.); gyluo@stu.xmu.edu.cn (G.L.); 23320231154461@stu.xmu.edu.cn (S.Z.);
[2] School of Information Science and Technology, Xiamen University Tan Kah Kee College, Zhangzhou 363123, China
[3] Navigation Institute, Jimei University, Xiamen 361021, China
[4] Department of Applied Informatics, Fo Guang University, Yilan 262307, Taiwan
[5] Department of Artificial Intelligence, Tamkang University, New Taipei City 25137, Taiwan
[6] Department of Electrical Engineering, National Dong Hwa University, Hualien 974301, Taiwan
* Correspondence: gaozhibin@jmu.edu.cn (Z.G.); hcchao@gmail.com (H.-C.C.)

Abstract

Federated learning (FL) has emerged as a promising paradigm for enabling collaborative training of machine learning models while preserving data privacy. However, the massive heterogeneity of data and devices, communication constraints, and security threats pose significant challenges to its practical implementation. This paper provides a system review of the state-of-the-art techniques and future research directions in FL, with a focus on addressing these challenges in resource-constrained environments by a cloud–edge–end collaboration FL architecture. We first introduce the foundations of cloud–edge–end collaboration and FL. We then discuss the key technical challenges. Next, we delve into the pillars of trustworthy AI in the federated context, covering robustness, fairness, and explainability. We propose a dimension reconstruction of trusted AI and analyze the foundations of each trustworthiness pillar. Furthermore, we present a lightweight FL framework for resource-constrained edge–end devices, analyzing the core contradictions and proposing optimization paradigms. Finally, we highlight advanced topics and future research directions to provide valuable insights into the field.

Keywords: federated learning; privacy-preserving AI; trustworthy AI; lightweight method; cloud–edge–end collaboration

Academic Editors: Dariusz Rzońca and Tomasz Rak

Received: 10 April 2025
Revised: 3 June 2025
Accepted: 18 June 2025
Published: 20 June 2025

Citation: Zhan, S.; Huang, L.; Luo, G.; Zheng, S.; Gao, Z.; Chao, H.-C. A Review on Federated Learning Architectures for Privacy-Preserving AI: Lightweight and Secure Cloud–Edge–End Collaboration. *Electronics* **2025**, *14*, 2512. https://doi.org/10.3390/electronics14132512

1. Introduction

1.1. Background and Overview

With the maturity and widespread application of 5G technology, both academic and industrial communities are looking forward to and exploring the vision of 6G networks, hoping to leverage their high bandwidth, ultra-low latency, and massive connectivity features to support various advanced application scenarios, including the Internet of Things (IoT) [1,2]. The core of 6G lies in the shift from "connecting everything" to "connecting intelligence". This transformation requires the integration of advanced AI algorithms and distributed computing capabilities. These technologies enable massive edge devices and terminals to collaboratively perform complex intelligent tasks [3].

At the same time, cloud computing has matured and plays an irreplaceable role in the era of big data. However, relying solely on centralized cloud computing cannot fully meet

the increasing demands in terms of bandwidth, privacy, and real-time requirements [4]. For this reason, edge computing has emerged, which deploys computing and storage resources closer to the data source at the network edge, thereby significantly reducing latency and bandwidth usage [5]. Nowadays, the collaboration between edge computing and end devices is also rapidly evolving, forming a "cloud–edge–end" multi-layer collaborative model:

- Cloud: It possesses centralized ultra-large-scale computing and storage resources, suitable for the training of complex models and massive data analysis.
- Edge: It has relatively limited but flexible deployment of computing nodes (e.g., base stations, roadside units, or micro data centers), which can provide low-latency services for applications with high real-time requirements [6].
- End: Refers to terminal devices (e.g., various IoT sensors, wearable devices, and intelligent vehicles), which are truly close to the data source and have a large quantity. They can operate lightweight AI models or participate in collaborative training under various scenarios [7,8]. A large number of research studies and practical applications have shown that a "cloud–edge–end" architecture can balance the needs for the global analysis of massive data and local real-time processing. It is widely used in scenarios such as autonomous driving, video surveillance, intelligent manufacturing, smart healthcare, and AI-generated content that demand high bandwidth, low latency, and computational capabilities [9–12]. Simultaneously, the emergence of distributed data and layered heterogeneous networks continues to drive the iteration of security and privacy protection technologies [13,14]. Therefore, under such developmental trends, the cloud–edge–end collaborative model provides a new direction for future intelligent applications.

Many applications (e.g., autonomous driving, telemedicine, and AR/VR) [15] are sensitive to end-to-end latency, and relying solely on centralized cloud computing will face problems such as network congestion, excessive transmission overhead, or long response times. Edge computing can provide nearby computing power support, completing some or all data processing at the network edge or terminal nodes, thereby reducing the overall latency and improving user experience [16,17].

With the exponential growth of video surveillance, industrial production data, and sensor data, if all data were to be transmitted back to the cloud, it would not only occupy the backbone network bandwidth but also lead to high energy consumption. Through the hierarchical division of labor from cloud to edge to end, computational tasks or caching strategies that consume a large amount of bandwidth can be pre-positioned to alleviate the transmission pressure on the core network [18].

However, while cloud–edge–end collaboration can significantly enhance system performance, resource utilization efficiency, and user experience, it also introduces critical privacy and security concerns due to decentralized data handling. Many types of data are sensitive (e.g., medical images, personal biological information, and vehicle driving data). In particular, the frequent exchange of sensitive data across distributed nodes raises substantial privacy leakage risks. To effectively address these emerging concerns, federated learning (FL) has become an increasingly prominent research direction due to its inherent capability to perform collaborative model training without directly transferring raw data from local nodes to a centralized server. Processing or collaborative training at the edge or end can effectively reduce cross-domain data transmission, thereby protecting user privacy and reducing compliance risks [19]. In the field of medical health, cloud–edge–end collaboration facilitates multi-party collaborative analysis and the rapid diagnosis of sensitive data [16]. In Vehicle-to-Everything (V2X), intelligent vehicles can cooperate with roadside units or nearby edge nodes to achieve low-latency decision-making and intelligent

scheduling [20]. In intelligent manufacturing, multiple devices or production lines can improve production efficiency through a combination of edge collaboration and cloud big data analysis [10]. FL, therefore, represents a promising solution to preserve data privacy while enabling effective cross-node collaboration within the cloud–edge–end architecture.

1.2. Motivation and Main Challenges

While cloud–edge–end collaborative architectures offer substantial benefits in terms of reduced latency, improved bandwidth efficiency, and enhanced real-time processing capabilities, their decentralized nature introduces prominent challenges, particularly concerning privacy, security, and system efficiency [21]. In traditional centralized machine learning or data mining frameworks, training data must be concentrated in the cloud, which not only poses a potential risk of privacy leakage but also conflicts with the compliance policies of an increasing number of industries.

Firstly, the decentralization of data processing inherently leads to increased exposure to potential privacy and security risks. Unlike centralized systems where data governance and security enforcement are straightforward, distributed environments require advanced privacy-preserving methodologies to ensure compliance with stringent data protection regulations. FL has emerged as a promising paradigm to conduct local training on mobile or edge nodes, uploading only model parameters or gradients to the cloud/edge aggregation, realizing the concept of "data 88 stays, models move" [22,23]. But effective FL requires robust methods for secure aggregation, differential privacy integration, and adaptive security protocols tailored to varying privacy sensitivity across domains.

Secondly, significant device and network heterogeneity, along with stringent resource constraints, exacerbate the complexity of deploying FL in cloud–edge–end scenarios:

- Device Capability Constraints: The computation, storage, and energy consumption of edge nodes or terminal devices are generally limited, making it difficult to run large-scale models or maintain long-term deep operations [24]. Especially in IoT scenarios, sensors, wearable devices, and the like often have extremely limited resources, requiring algorithms to be lightweight or scalable while ensuring accuracy [25].
- Network Instability and Connectivity Issues: The number of edge devices connected in real time is vast, and their conditions are variable. Some devices or edge nodes may frequently go offline or experience communication delays or packet loss because of insufficient bandwidth [9]. This dynamism affects the convergence efficiency of FL and distributed training, which requires the development of adaptive collaboration strategies.
- Data Heterogeneity (i.e., Non-Independent and Identically Distributed, non-IID): Compared to traditional centralized training, data in the cloud–edge–end scenario often exhibits non-IID characteristics. Different edges or terminals exhibit significant differences in data categories, distribution, and quantity, which can easily lead to unstable model training or a decline in performance [19]. How to design robust federated optimization algorithms and adaptive aggregation strategies is crucial for the overall performance of the system.

Lastly, integrating trustworthy AI principles—such as robustness, fairness, explainability, and accountability—into FL systems significantly enhances their dependability but simultaneously introduces additional complexity and computational overhead. Balancing these trustworthiness attributes against the practical limitations of resource-constrained edge and end nodes remains a fundamental yet unresolved challenge.

Addressing these intertwined challenges—privacy and security risks, device and network heterogeneity, resource constraints, and trustworthiness integration—motivates this systematic review. Our work aims to critically assess current strategies, identify

knowledge gaps, and propose potential research directions to realize efficient, secure, and trustworthy FL within cloud–edge–end collaborative environments.

1.3. Summary of Contributions

This paper presents a comprehensive and systematic review of FL architectures tailored for privacy-preserving AI in cloud–edge–end collaboration environments. We explore a cloud–edge–end collaboration FL framework, emphasizing vertical functional decoupling and horizontal resource complementarity. A three-dimensional trustworthiness framework is then reconstructed for FL, encompassing data trustworthiness, process trustworthiness, and outcome trustworthiness. Through a comprehensive analysis, we aim to provide insights into how cloud–edge–end collaboration FL can be implemented to be lightweight, trustworthy, and secure in resource-constrained environments.

1.4. Review Structure

This review is structured as follows: Section 2 provides our research questions and a detailed account of the literature collection process, including search terms, eligibility criteria, and the evaluation methodology. In Section 3, we systematically investigate the cloud–edge–end collaborative architecture and its implementation challenges, covering hierarchical computing paradigms, technical bottlenecks, and communication constraints. We also explore potential solutions for secure multi-layer collaboration. In Section 4, we present the integration of FL with trustworthy AI principles, analyzing robustness foundations, redefining fairness dimensions, and establishing explainability pillars. In Section 5, we dissect the core contradictions in resource-constrained environments through the trilemma analysis of privacy–efficiency–accuracy trade-offs. We also explore the optimization paradigms for FL with resource constraints. Finally, in Section 6, we discuss current advanced topics and propose future research directions.

2. Research Methodology

2.1. Research Goal Formulation

We aim to conduct an in-depth and systematic review of FL architectures tailored for privacy-preserving AI within cloud–edge–end collaborative environments. Given the increasing complexity of intelligent systems and the urgent need for secure and efficient decentralized learning, this review is structured around the following research goals:

- **RQ1**: What are the state-of-the-art architectures for privacy-preserving FL in cloud–edge–end collaborative environments, and how are they categorized based on deployment patterns, coordination mechanisms, and communication structures?
- **RQ2**: What are the major technical challenges and trustworthiness concerns—such as robustness, fairness, explainability, and security—in these architectures, and what methods have been proposed to address them?
- **RQ3**: What future research directions and open opportunities exist for enabling lightweight, secure, and trustworthy FL under dynamic and resource-constrained cloud–edge–end conditions?

2.2. Systematic Literature Review Approach

A systematic literature review is a rigorous and structured method that integrates and evaluates the available research on a specific topic. Following guidelines such as PRISMA [26], researchers can locate relevant studies systematically, assess the strength of their evidence critically, and combine key results to address a specific research question. This process involves data extraction and quality assessment to collect essential information and ensure reliability. The analysis then categorizes and summarizes the primary

conclusions. Ultimately, the findings are interpreted in relation to the research focus, with a discussion of the implications, limitations, and potential directions for future research. This thorough evaluation of the literature provides not only a transparent assessment of the current evidence base but also advances scientific knowledge and supports evidence-based decision-making.

Step 1: Data processing search and selection

The data processing phase in a systematic literature review consists of a series of steps. These steps aim to identify relevant studies and select those that align with the predefined inclusion criteria ensuring the coherence between the chosen studies and the research objectives. The following link provides an overview of this data search process:

1. IEEE Xplore digital library (https://ieeexplore.ieee.org, accessed on 17 January 2025).
2. Elsevier ScienceDirect (https://www.sciencedirect.com, accessed on 17 January 2025).
3. Web of Science (https://webofscience.clarivate.cn, accessed on 17 January 2025).

The review's temporal scope spans from 2021 to January 2025, which was deliberately selected to capture the latest advances in federated learning architectures, particularly in light of the widespread adoption of cloud–edge–end paradigms and the integration of privacy-preserving mechanisms such as differential privacy, secure aggregation, and the blockchain. However, we acknowledge that this temporal delimitation may exclude influential foundational works published prior to 2021. While our review prioritizes recent developments that reflect the current state and trends of the field, earlier contributions—especially those from 2017 to 2020—played a crucial role in shaping the trajectory of FL. As such, this scope constitutes a limitation of the present study, and we encourage readers to consult complementary reviews covering earlier periods for historical grounding. The search in both databases employed a specific set of keywords: ((“federated learning”) AND (“cloud–edge–device” OR “device–edge–cloud” OR “cloud–edge” OR “end–edge–cloud” OR “edge–cloud”)).

Step 2: Requisites for inclusion and exclusion

In addition, we formulated the inclusion and exclusion criteria for the literature according to the research topic of this review:

- Requisites for inclusion:

1. Technical Relevance
    - Studies proposing architectures, algorithms, or frameworks for privacy-preserving FL in cloud–edge–device collaboration (e.g., split learning and encrypted aggregation).
    - Works addressing resource constraints (e.g., computational efficiency, communication optimization) through lightweight model design, adaptive offloading, or dynamic resource allocation.
    - Research integrating trustworthy AI principles (robustness, fairness, and explainability) into FL workflows, particularly in distributed environments.
2. Application Context
    - Papers validating solutions in key application domains or analogous scenarios requiring multimodal data fusion or real-time decision-making.
3. Methodological Rigor
    - Empirical studies with quantitative evaluations (e.g., accuracy, latency, and privacy leakage metrics) and comparisons against baseline methods.
    - Theoretical analyses provide convergence guarantees, privacy bounds, or scalability proofs for the proposed algorithms.
4. Publication Quality and Academic Influence

- Studies published in reputable, peer-reviewed venues indexed by IEEE Xplore, ScienceDirect, and Web of Science, ensuring a baseline level of editorial and methodological rigor.
- Preference was given to highly cited works within the domain of federated learning and cloud–edge–end collaboration, using the citation count as a secondary indicator of reliability and relevance.

5. Temporal Scope

   - Publications from 2021 to 2025 (January).

However, the query terms yielded many irrelevant results, with some papers mentioning FL only briefly within unrelated contexts. Our exclusion criteria are listed below:

- Requisites for Exclusion:

1. Initial Screening of Title

   - Further excluding the literature that does not contain keyword combinations relevant to the search.

2. Scope Misalignment

   - Studies focused solely on centralized cloud computing or standalone edge/device architectures without cross-layer collaboration.
   - Works on FL in non-distributed environments (e.g., single-server/client setups) that lack explicit privacy-preserving mechanisms.

3. Methodological Deficiencies

   - Conceptual papers without experimental validation or theoretical grounding.
   - Redundant studies replicating existing frameworks without novel contributions (e.g., incremental parameter tuning of FedAvg).

4. Contextual Irrelevance

   - Applications unrelated to cloud–edge–end ecosystems.
   - Non-English publications or non-peer-reviewed technical reports.

It should be noted that, despite following a structured and systematic review process, certain methodological limitations remain. First, the reliance on a limited number of databases (IEEE Xplore, Web of Science, and ScienceDirect) may result in selection bias, potentially omitting relevant studies published elsewhere. Second, the chosen search terms, though representative, may miss papers that adopt alternative terminologies. Third, while clear inclusion and exclusion criteria were applied, the interpretation of borderline cases inevitably introduces subjectivity. These limitations may affect the completeness and generalizability of the findings and should be considered when interpreting the conclusions.

Step 3: Literature selection process

The literature screening flowchart, illustrated in Figure 1, outlines a transparent and reproducible method for reporting the search and selection process.

Initially, the search strategy was executed across several databases retrieving 1575 papers. Of these, 1271 papers were from IEEE Xplore, 262 papers were from Web of Science, and 42 papers were from Elsevier ScienceDirect to ensure comprehensiveness. After the initial collection, a duplicate removal process was performed that removed 10 duplicate papers. This step yielded 1565 unique articles that met the conditions for subsequent filtering. Each of the 1565 articles was meticulously evaluated based on predefined eligibility criteria, and their titles and abstracts were thoroughly reviewed. As a result, 1467 papers were excluded for not meeting the criteria or for being identified as review-type articles. This careful filtering process resulted in the final selection of 98 articles for an in-depth full-text

review, ensuring that only the most relevant and high-quality studies were considered for further analysis. Figure 2 illustrates the annual distribution of the included papers.

Step 4: Data extraction, synthesis, and analysis

After the inclusion of the final 98 articles, we implemented a structured qualitative synthesis to extract thematic insights and generate an organized review framework. A standardized data extraction table was constructed to record six key attributes from each study, including the following: (1) the proposed FL architecture, (2) deployment layer(s) (cloud, edge, or end), (3) privacy-enhancing techniques, (4) lightweight technology, (5) application scenarios, and (6) reported challenges and solutions.

These six attributes were further grouped based on thematic similarities into higher-level categories such as system architecture, security/privacy mechanisms, and optimization strategies, which structured the major sections of our review.

Regarding the differences in the research results, they were addressed by contextualizing them within the application domain or deployment scale and noting explicitly where necessary. When conflicting results arose, we emphasized common conditions or assumptions behind each study to preserve clarity.

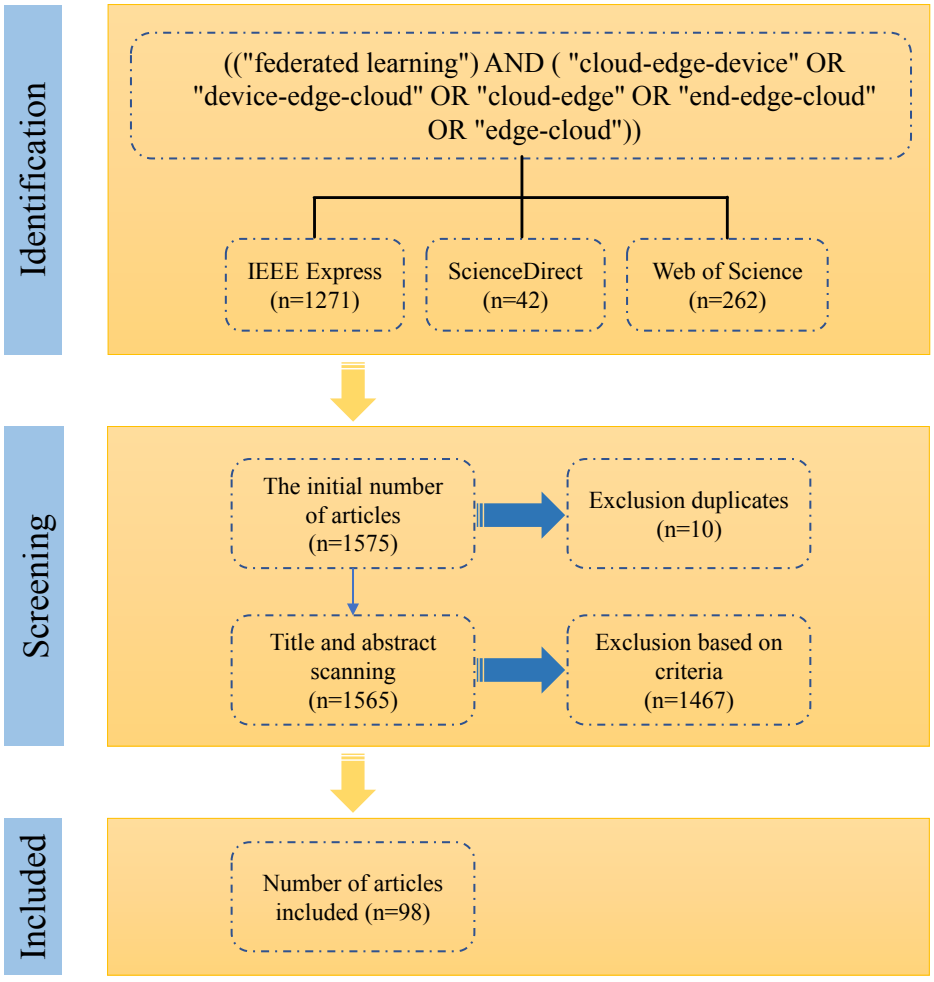

Figure 1. The literature review in this study employs a structured approach to article retrieval, consisting of three distinct phases: identification, screening, and inclusion.

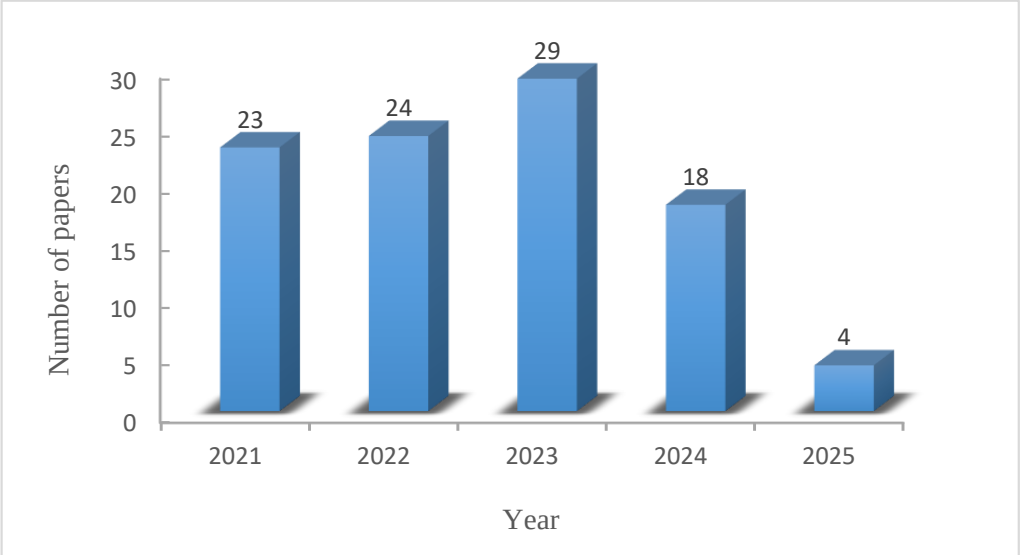

Figure 2. The number of included papers per year.

3. Cloud–Edge–End Collaboration: Architecture, Challenges, and Privacy–Security Concerns

3.1. Multi-Layer Architecture and Function

3.1.1. Hierarchical Collaboration Concept

By combining vertical function separation with horizontal resource sharing, the hierarchical architecture provides a scalable framework for distributed collaboration. While related paradigms such as fog computing also address distributed intelligence [18], this review focuses on the cloud–edge–end architecture due to its widespread adoption in the recent FL literature and clearer three-layer decoupling. In a cloud–edge–end collaborative system, the architecture typically consists of three layers: the cloud layer, edge layer, and end layer. Each layer has specific functions tailored to the requirements of modern computing and communication systems. The cloud layer handles global model aggregation and centralized resource scheduling, leveraging its large-scale processing and storage capabilities. The edge layer is closer to the terminal devices, providing real-time preprocessing functions, ensuring lower latency and less communication overhead, and coordinating real-time data processing and local model optimization within the region. Terminal devices (including IoT devices, smartphones, and wearable devices) are responsible for local inference and micro-training, performing model updates based on locally collected data, forming a "centralized–coordinated–execution" three-level collaborative closed loop.

- Cloud Layer: Global Computation and Model Aggregation Center
  The cloud layer serves as a top-level hub, relying on powerful computing and storage capabilities to undertake global model training, parameter aggregation, and strategy scheduling tasks. Reference [27] proposed the FedAgg framework, which, through a recursive knowledge distillation protocol, achieves layer-by-layer model expansion from the edge to the cloud, enhancing generalization performance while satisfying privacy constraints. The SFETEC framework [28] further decomposes the model into "base–core" components, allowing the cloud to centrally optimize core model parameters, significantly reducing the cross-layer communication load. Moreover, by integrating local updates from multiple edge nodes (e.g., clustered federated architecture [29]), the cloud layer can effectively alleviate data heterogeneity issues, enhancing the robustness of the global model. Reference [30] introduced a layered FL system that employs a federated averaging strategy at the edge–cloud layer, optimizing user–edge allocation relationships to make the data distribution at the edge layer approach

independent and identically distributed (IID), thereby improving the global model performance. Similarly, the CEE-FLA architecture [31] moves the traditional model aggregation task from the cloud to the edge layer, reducing the frequency of direct edge–cloud connections, while employing a K-Vehicle random scheduling strategy to mitigate the impact of edge–side heterogeneity on the convergence speed.

- Edge Layer: Real-time Collaboration and Resource Scheduling Hub
  The edge layer acts as an intermediate bridge between the cloud and edge, possessing both a low-latency response and regional coordination capabilities. It mainly performs data preprocessing, local model aggregation, and dynamic resource allocation. Reference [32] proposed the I-UDEC framework, which integrates the blockchain and AI to achieve the joint optimization of computation offloading and service caching in ultra-dense 5G networks, balancing real-time performance and security. The clustered federation mechanism [33] balances the communication efficiency between edge nodes and model convergence speed through a layered asynchronous aggregation strategy. The HybridFL protocol [34] adopts an "edge–cloud" two-level aggregation strategy: the edge layer introduces a "regional relaxation factor" through a probabilistic client selection mechanism to alleviate device dropout and performance fluctuation issues, whereas the cloud layer performs asynchronous global updates to shorten the duration of federation. The FED GS framework [35] further exploits the natural clustering properties of factory equipment, constructing homogeneous super-nodes through a gradient replacement algorithm, and deploying a composite step synchronization protocol at the edge layer to enhance robustness against non-IID data. The edge layer can also serve as an implementation carrier for incentive mechanisms. The evolutionary game model [36] optimizes the enthusiasm for edge node participation by dynamically adjusting the cluster reward strategies.
- End Layer: Privacy Protection and Lightweight Execution
  End devices, serving as data sources and lightweight computation units, focus on local model inference or fine-tuning and reduce the transmission of raw data or transmit encrypted data. The FedHome framework [37] generates a balanced dataset while protecting user privacy through a generative convolutional autoencoder (GCAE) at the edge side, alleviating the problem of non-IID data in medical monitoring scenarios; FedSens [38] further addresses the challenge of class imbalance in health monitoring, proposing a lightweight federated optimization algorithm that adapts to the resource constraints of edge devices. Moreover, the edge side can indirectly participate in global training through the edge layer. FedParking [39] proposed leveraging the idle computing power of parking terminals to perform federated tasks and coordinate model updates through edge servers, thereby achieving dual improvements in resource utilization and privacy protection. The FedVL framework [40] implements personalized federated learning (PFL) at the edge side, collaboratively training adaptive models in cloud–edge–end scenarios, and utilizing semi-supervised mechanisms to cope with dynamic environmental changes. The Blockchain Federated Learning (BFL) architecture [41] allows mobile devices to offload data to edge servers and achieves decentralized model aggregation through P2P blockchain communication, resisting poison attacks.

The efficiency of the layered architecture relies on the innovative design of the cross-layer collaboration mechanisms:

- Computation Collaboration: The cloud layer and edge layer achieve dynamic adaptation of heterogeneous computing resources through model segmentation [28] or distillation [27]. Reference [41] proposed a joint optimization scheme based on deep reinforcement learning (DRL) to dynamically adjust the computation resource allocation

and channel the bandwidth of mobile devices. The K-Vehicle scheduling strategy [31] reduced the negative impact of low-performance devices on model convergence by randomly selecting high-computation vehicles for training. Both the DQN-driven parameter pre-synchronization in [42] and the composite step synchronization protocol in [35] reflect the evolution trend from static resource allocation to dynamic adaptive allocation.

- Communication Optimization: The edge layer reduces the pressure of direct end-to-cloud transmission by utilizing cluster aggregation [33], asynchronous updates [32], or privacy relaying [39]. The PSPFL framework [42] introduced parameter selection and pre-synchronization mechanisms at the edge–end layer. The clients only transmit partial key parameters, and the edge base station performs pre-aggregation before uploading to the cloud, significantly reducing the amount of data transmitted. Reference [30] optimized the user–edge allocation relationship, making the data distribution at the edge layer approach IID, thus reducing the number of rounds required for global aggregation. Meanwhile, reference [34] probabilistically selected clients, and [41] used blockchain P2P communication to optimize communication efficiency from device reliability and security perspectives, respectively.
- Security Enhancement: The edge adopts local data retention strategies [37,38], the edge layer introduces anonymization and incentive mechanisms [36], and the cloud layer implements encrypted aggregation [27], constructing a multi-level defense system. The BFL framework [41] combines blockchain consensus mechanisms with FL. Through hash power allocation and data offloading decision optimization, the trustworthy verification of model sharing and rapid detection of poison attacks are achieved. The FED GS framework in [35] employs gradient permutation algorithms at the edge layer to avoid the risk of exposing sensitive industrial data during super-node construction. In contrast, reference [34] mitigated device unreliability through relaxation factors, whereas reference [40] isolated private data through personalized models, reflecting different security design emphases at various levels.

Furthermore, a layered collaborative design needs to adapt to the differentiated requirements of various application scenarios:

- Highly Dynamic Scenarios: Reference [32] supported the rapid processing of vehicle perception data and model updates through an intelligent ultra-dense edge computing framework, combined with real-time resource allocation algorithms. The CEE-FLA architecture [31] uses edge servers as regional aggregation centers, designs random scheduling strategies considering the performance differences of vehicles, and supports the rapid processing of highly dynamic vehicle data. Reference [40] further realized personalized positioning in multiple scenarios through cloud–edge–end collaboration, addressing model drift issues caused by changes in the vehicle environment.
- Strong Privacy Scenario: References [37,38] proposed generative data augmentation and class balancing strategies, respectively, to improve model accuracy while avoiding the sharing of original medical data. The FED GS framework [35] targeted the characteristics of factory equipment clusters, utilized gradient replacement algorithms to construct homogeneous super-nodes, and addressed dynamic stream data and non-IID through edge layer synchronization protocols, thereby adapting to high real-time, strong privacy industrial requirements.
- Large-scale Node Scenarios: References [29,33] addressed the efficiency and stability issues of training caused by massive terminals through data clustering and cluster federation mechanisms. The BFL framework [41] achieved low-latency, anti-attack model training in edge computing scenarios through blockchain consensus mechanisms and joint optimization algorithms, addressing sensitive data sharing in smart cities.

3.1.2. Cloud–Edge–End Collaborative Architecture in Internet of Vehicles (IoV)

The IoV, as the core scenario of intelligent transportation systems, relies highly on the collaborative architecture of the cloud, edge, and end for real-time perception, massive node management, and resource optimization.

The traditional vehicle communication network architecture relies on "end–cloud" single-layer interaction, which leads to high computational pressure on vehicle terminals and high communication latency in the cloud. The cloud–edge–end collaborative architecture introduces an edge layer to achieve hierarchical task processing and dynamic resource scheduling. For example, reference [31] proposed a CEE-FLA model based on a cloud–edge–end dual-layer architecture, which moved model aggregation tasks from the cloud to edge servers and reduced the number of cloud communications, while using a K-Vehicle random scheduling strategy to alleviate performance differences in vehicles. Furthermore, reference [11] designed a two-layer FL model in 6G ultra-dense networks, utilizing edge servers (RSU) to aggregate local models, thereby reducing the response latency of autonomous driving target detection tasks. Such designs highlight the core value of the edge layer in the real-time response and computational load diversion.

The dynamism and resource constraints of the vehicle network scenario require the edge layer to have elastic scheduling capability. Reference [43] proposed the FLOR framework, integrating V2X, 5G-mmWave, and 6G-V2V heterogeneous networks, calculating the upper limit of communication delay through stochastic network calculus, and dynamically allocating wireless resources based on federated Q-learning, thereby improving the efficiency of task offloading. In response to the interruption of edge coverage caused by vehicle mobility, reference [44] designed an asynchronous federated learning-driven CAFR scheme that combines DRL to dynamically adjust the RSU caching strategy, improve the cache hit rate, and reduce the model update loss caused by vehicles leaving. Such research verifies the irreplaceability of the edge layer in terms of resource elasticity scheduling and mobility adaptation.

The cloud–edge architecture achieves collaborative optimization of data security and computational efficiency through embedded privacy protection mechanisms. Reference [45] utilized edge servers to realize the collaborative positioning of vehicles and protect trajectory privacy through FL. Reference [46] further proposed the FedSLT algorithm, which reduced the burden on wireless links and enhanced model training speed in heterogeneous scenarios through selective layer transmission and customized parameter initialization at the edge layer. Reference [47] designed a context clustering FL framework based on the Siamese Neural Network (SNN) for trajectory prediction needs of autonomous driving vehicles (CAVs). By grouping clients for training based on static environmental similarities, the risk of privacy leakage was reduced. This indicates that FL, as an instrumental technology, can be embedded in the cloud–edge architecture to optimize global efficiency without sacrificing privacy.

The cloud–edge–end collaborative architecture in the IoV provides an expandable technical foundation for intelligent transportation systems through layered decoupling (e.g., cloud global scheduling, edge real-time processing, and end lightweight computing), dynamic resource adaptation (e.g., heterogeneous network integration and asynchronous caching), and privacy–efficiency balance. In the future, further exploration is needed in edge intelligence enhancement and ultra-low latency protocol design to meet the extreme demands of scenarios such as autonomous driving.

3.1.3. Cloud–Edge–End Collaborative Architecture in Smart City

Countless IoT devices are scattered across urban areas, and as a typical scenario of massive node collaboration and real-time response, the collaboration between the cloud,

edge, and end helps manage the data of these devices while ensuring privacy and scalability. Edge nodes play a crucial role in processing massive amounts of real-time sensor data and reducing the latency required for intelligent urban management. The cloud–edge–end collaborative architecture in smart cities provides an expandable technical foundation for massive node collaboration through real-time resource scheduling [32,48], privacy protection embedding [49,50], and dynamic model optimization [51].

The massive number of IoT devices and the dynamic network environment in smart cities pose challenges for real-time resource scheduling. Reference [32] proposed an I-UDEC framework that integrates the computing, communication, and storage resources of 5G networks. Dual-timescale deep reinforcement learning (2Ts-DRL) jointly optimizes computation offloading and resource allocation, reducing the task execution time by 31.87%. Similarly, reference [48] deployed AI-empowered MEC servers in Vehicular Edge Networks (VENs), combining deep Q-networks with FL to achieve dynamic data sharing, reducing data update latency by 25%. Such solutions validate the core value of the edge layer in real-time response and heterogeneous resource integration.

Data privacy is a core constraint in the large-scale node collaboration of smart cities. Reference [49] proposed a traffic flow prediction model based on a federated spatio-temporal network (FedSTN), which shares short spatio-temporal hidden information through Vertical FL in an encrypted manner. While protecting trajectory privacy, its prediction accuracy increased by 18% compared with the centralized models. Reference [50] further designed an edge–cloud collaborative FL mechanism to achieve local model training and edge aggregation in traffic vehicle identification scenarios. The risk of privacy leakage was reduced by 30%, and the detection latency decreased by 22%.

In addition, the dynamism and heterogeneity of smart city scenarios require a cloud–edge–end architecture to exhibit elastic adaptability. The I-UDEC framework [32] implemented the distributed training of 2Ts-DRL models through FL and ensured the security of resource allocation strategies by combining blockchain technology. Reference [51] proposed a cloud–edge collaborative fine-tuning framework for power grid scenarios using reinforcement learning (RL) to dynamically segment models and filter unreliable samples. Such research highlights the necessity of edge intelligence and dynamic task offloading in complex urban systems. To cope with the extreme demands of large-scale urban systems, further exploration of federated collaboration between edge nodes and cross-domain resource pooling is required.

3.1.4. Cloud–Edge–End Collaborative Architecture in Healthcare

Healthcare, as a typical scenario that is sensitive to privacy and requires collaboration among multiple institutions, also relies on the support of a cloud–edge–end collaborative architecture for data privacy protection, heterogeneous resource integration, and dynamic model optimization.

The sensitivity of medical data requires strict restrictions on the cross-institutional sharing of the original data. The FedHome framework [37] generated balanced datasets at the edge side through GCAE, solving the non-IID problem of user health data. For the scenario of COVID-19 diagnosis, reference [52] designed the FedGAN framework, combining Generative Adversarial Networks (GANs) with differential privacy (DP) technology to generate synthetic medical imaging data at the edge side to avoid uploading patients' raw data. This confirms the dual value of edge generative learning for privacy protection and data enhancement.

Cross-institutional medical collaboration must address the contradiction between data heterogeneity and model generalization. Reference [53] proposed a COVID-19 diagnostic framework based on clustered federated learning (CFL), which trains multimodal imaging

models in groups on edge servers and improves the F1-score by 16% and 11% on X-ray and ultrasound datasets, respectively, compared to centralized baselines. Reference [54] further designed a semi-supervised FL framework, Fedsemgan, which, under the mixed scenario of "edge annotation" and "cloud annotation", integrates unlabeled pathological data using GAN and reduces gradient diversity through the Regrouping Averaging strategy. Such research indicates that edge-driven heterogeneous data fusion can overcome the limitations of single-institution data.

The dynamism of medical scenarios requires that models respond quickly and update adaptively. Reference [55] proposed a real-time prediction framework based on Federated Logistic Regression (FLR), which improves model reliability and efficiency by collaboratively optimizing loss functions and gradient computations between the cloud and edge. FedHome [37] utilized a lightweight model transmission mechanism to reduce bandwidth occupancy in cloud–edge communication. This highlights the necessity of dynamic task offloading and lightweight edge protocols in real-time medical decision-making. Reference [56] further supports this architecture by employing a three-layer edge–fog–cloud system with NB-IoT for remote health monitoring, achieving over a 50% reduction in delay and execution time. This validates the benefits of distributed processing and lightweight protocols for real-time, privacy-preserving medical analytics.

3.2. Key Technical Challenges

3.2.1. Data Distribution and Heterogeneity

In an IoT environment, the heterogeneity of hardware devices, network architectures, and data modalities significantly increases the training and inference complexity of cloud–edge–end collaborative intelligent systems. Data generated from different devices (e.g., industrial sensors, vehicle terminals, and medical equipment) exhibit high heterogeneity in formats (e.g., images, time-series signals, and text) and distributions, and there is a prevalent phenomenon of non-IID data. In industrial scenarios, the data loss patterns of different factories differ significantly [57], and in network traffic anomaly detection, the data distribution of edge nodes may change dynamically because of the region or protocol type [58]. Traditional FL methods (e.g., FedAvg [3]) are prone to issues like model divergence or performance degradation in such heterogeneous environments [59], mainly due to their strong assumptions about data distribution and the limitations of static weight allocation strategies.

In recent years, researchers have proposed multi-level solutions to address this challenge. At the algorithm level, the FedCD framework enhances the local training process by integrating personalized knowledge from similar clients through a cross-client knowledge distillation mechanism. It also designs dynamic aggregation weights based on client correlations, achieving a 16.65% improvement in model testing accuracy in non-IID scenarios [59]. In terms of data preprocessing, the FedTMI method innovatively combines Generative Adversarial Imputation Nets (GAIN) with transfer learning and utilizes edge knowledge vectors to screen auxiliary models, effectively addressing the adaptation challenges of data interpolation in cross-factory settings [57]. Moreover, for dynamic network environments, the IFCEA algorithm selects unbiased data clusters through a device–side committee mechanism and optimizes the federated clustering process with distribution-balanced weights, enhancing anomaly detection accuracy [58]. Despite these significant advancements, adaptability in dynamic environments remains a core bottleneck. For instance, the static knowledge distillation strategy of FedCD struggles to capture the temporal variations in data distribution, while the transfer rules of FedTMI in new protocol scenarios still need optimization. Exploring meta-learning-driven dynamic knowledge transfer mechanisms

combined with real-time data evolution capture through online clustering techniques can further enhance model robustness in heterogeneous environments.

3.2.2. Communication Overhead and Latency Sensitivity

In cloud–edge–end collaborative systems, the communication overhead and network latency caused by the participation of massive devices have become a key bottleneck restricting the scalability of the system. In typical scenarios such as network traffic classification tasks, traditional centralized training requires uploading TB-level traffic data to the cloud, causing imbalanced bandwidth utilization between the edge and end and a surge in transmission latency [60]. Moreover, dynamic network conditions (e.g., vehicles frequently switching base stations in vehicular networks) may lead to up to a 50% gradient transmission packet loss, seriously undermining the stability of model convergence.

The current research addresses this challenge from two dimensions: architectural optimization and resource scheduling. In terms of architectural design, the Hier-SFL algorithm innovatively combines split learning with FL. Through a three-tier computing task allocation mechanism of client–edge–cloud, it compresses the dimensionality of intermediate features that end devices need to transmit, achieving a significant improvement in communication efficiency on the CIC-IDS2018 dataset [60]. At the resource scheduling level, the AUCS algorithm introduces an online auction mechanism based on combinatorial multi-armed bandits, utilizing the Upper Confidence Bound (UCB) to dynamically select high-cost-effective edge nodes for aggregation, reducing overall training latency and ensuring model convergence theoretically [61]. Moreover, addressing the uncertainty of data collection, the dual-timescale Lyapunov optimization strategy coordinates long-term planning with short-term decision-making, reducing the data acquisition cost of FL while minimizing end-to-end transmission delay [62]. It is worth noting that many existing methods assume the network bandwidth exhibits static or quasi-static variations. However, in actual industrial IoT environments, sudden traffic surges might lead to instantaneous congestion. Therefore, there is an urgent need to develop dynamic bandwidth prediction models based on DRL, combined with priority queue management and sparsified gradient transmission techniques, to achieve real-time optimization of network resource allocation. Additionally, attention should be given to the collaborative design of edge caching technology and model compression algorithms, such as using knowledge distillation to produce lightweight model replicas and pre-distributing them to edge nodes, further alleviating the transmission pressure on the core network.

3.2.3. Resource and Computational Constraints

The contradiction between the limited resources of edge devices (e.g., embedded GPU computing power and battery capacity) and the computational demands of complex models is becoming increasingly acute. Mobile devices participate in FL [63], while the privacy computing needs of medical terminals further exacerbate the energy consumption issue [64].

The current research addresses this challenge through cross-level resource collaboration and privacy–energy efficiency joint optimization. In terms of energy efficiency management, the Eco-FL framework introduces an entropy-driven device selection mechanism that takes into account both data information entropy and remaining power status, reducing energy consumption [65]. For computation-intensive tasks, the EAFL+ architecture innovatively introduces a three-level computing offloading strategy for cloud–edge–terminal, utilizing edge FPGAs to accelerate convolution operations, shortening the training time for mobile devices, and reducing the client dropout rate to zero [63]. In the dimension of privacy protection, the UIFLPP scheme divides the model into lightweight sub-modules on

the edge side and residual modules on the edge, combined with matrix masking and Laplacian noise injection, increasing the training speed by 5% under the premise of ensuring DP [64]. However, existing resource scheduling strategies are mostly based on static device capabilities and are difficult to adapt to dynamic load changes. Therefore, there is an urgent need to build an adaptive resource allocation framework that senses multimodal state parameters such as device computational load and temperature in real time and establishes a multi-objective optimization model for energy consumption, accuracy, and privacy.

3.2.4. Scalability and System Reliability

The dynamic network topology (e.g., the temporary networking of drone swarms) and intermittent online devices (e.g., shared cars entering or leaving service areas) pose severe challenges to system robustness. Traditional centralized architectures risk single-point failures, while the failure of edge nodes might lead to the accumulation of regional model biases.

Cutting-edge research enhances system reliability from two aspects: distributed architecture and fault tolerance mechanisms. In terms of architectural innovation, the FL system based on IOTA Tangle uses a directed acyclic graph (DAG) to store model shards and implements decentralized auditing through the IPFS network [66]. At the cloud computing platform integration level, the kubeFlower operator injects differential noise into stored data through the privacy-preserving persistent volume (P3-VC) mechanism, combined with the Kubernetes namespace isolation strategy, ensuring FL privacy while achieving multi-tenant secure collaboration [67]. For edge layer reliability, the MultiFed framework sinks aggregation servers to the edge, establishing a regional multi-center training architecture, and reduces communication latency for quality of service prediction tasks through dual gradient aggregation [68]. However, existing fault tolerance mechanisms mainly address device-level random failures and lack effective defense against collaborative attacks. It is necessary to build a collaborative defense system combining hardware-level trusted execution environments (TEEs) with blockchain smart contracts to achieve real-time verification and post-event auditing of model updates.

The technical challenges of the collaborative intelligent system at the edge of the cloud present multi-dimensional coupling characteristics, which need to be addressed through the cross-layer collaborative innovation of algorithms, architecture, and hardware. Although existing research has made breakthroughs in PFL, layered communication optimization, and dynamic resource scheduling, there are still theoretical gaps in adaptability to complex dynamic environments, the balanced optimization of security–efficiency–privacy, and the integration of new computing paradigms.

3.3. Privacy and Security Threats

3.3.1. Data Leakage Risks

Data leakage remains a critical concern, particularly in decentralized systems where local models are exchanged between the cloud, edge, and end devices. Without adequate encryption or secure aggregation methods, malicious actors can potentially intercept model updates or gradients, compromising sensitive information. Intermediate transmissions (e.g., gradients and model updates) are vulnerable to eavesdropping or adversarial reconstruction attacks.

In cloud–edge collaborative systems (e.g., the IoV), edge servers (ESs) handle latency-sensitive tasks but face challenges in securely deploying services. As noted in [69], FL combined with homomorphic encryption (HE) provides a solution by enabling ESs to exchange model weights instead of raw data. This approach reduces privacy leakage risks during service deployment decisions. However, even encrypted model parameters may

expose data patterns through gradient inversion attacks [70]. To address this, ref. [71] proposed a privacy-enhanced FL framework that splits models between clients and edge servers. By limiting gradient exposure to partial layers, attackers face computational barriers in reconstructing raw data.

Further defenses include DP mechanisms. For example, reference [72] introduces local differential privacy (LDP) to perturb model parameters before aggregation, achieving adjustable privacy guarantees. Similarly, reference [73] implemented a two-stage DP framework where edge servers inject noise into local models while user terminals perturb feature data. These layered protections mitigate risks but introduce trade-offs between privacy and model accuracy. Challenges persist in balancing communication overhead, computational costs, and privacy levels, especially for resource-constrained edge devices [70]. Future research directions include lightweight encryption protocols and adaptive privacy budgets tailored to dynamic edge environments.

3.3.2. Poisoning Attacks and Adversarial Samples

Malicious devices can inject harmful updates into the training process, resulting in compromised models or faulty predictions. These attacks can range from data poisoning to model inversion, where attackers extract private data by exploiting model weaknesses. Malicious nodes inject manipulated updates (e.g., label-flipping and backdoor triggers) to corrupt global models.

Poisoning attacks in the edge–cloud architecture manifest in two forms: data poisoning (manipulating training data) and model poisoning (tampering with uploaded gradients). As highlighted in [70], adversaries or "honest but curious" edge servers may launch label-flipping attacks or embed backdoor triggers during local model training. For instance, reference [74] demonstrated a stealthy clean-label attack in edge–cloud FL, where perturbations are added to gradients to bypass Byzantine-robust aggregation defenses. This attack achieves a 30 dB peak signal-to-noise ratio (PSNR) in poisoned images, evading detection while maintaining high attack success rates.

Defense strategies focus on anomaly detection and robust aggregation. Reference [75] proposed a partial cosine similarity (PCS) mechanism to filter malicious clients in hierarchical FL architectures. By analyzing gradient direction deviations, PCS identifies adversarial updates with minimal computational overhead. Meanwhile, reference [76] combined semi-supervised FL with network softwarization for intrusion detection systems (IDSs), achieving 84% accuracy in identifying poisoned data flows. However, existing methods struggle against advanced adaptive attacks that mimic legitimate gradient patterns [70]. Future work should explore hybrid approaches, such as integrating zero-knowledge proofs for update verification and leveraging a digital twin (DT) to simulate attack scenarios in edge environments [71].

3.3.3. Systemic Vulnerabilities

The security of edge devices is often overlooked, which makes them easy targets for physical layer or system layer attacks. With the increasing deployment of IoT devices at the edge, the attack surface grows, making it more difficult to defend against sophisticated cyberattacks. Weak security protocols on edge devices expose systems to physical tampering or firmware exploits.

Edge devices in the industrial Internet of Things (IIoT) and mobile networks face unique risks due to limited computational resources and heterogeneous architectures. Reference [77] identifies vulnerabilities in edge-based IDSs, where attackers exploit weak authentication protocols to inject false data. To mitigate this, the LocKedge framework

combines lightweight anomaly detection algorithms (e.g., decision trees) with FL-enabled collaborative learning.

Furthermore, physical attacks further compound these risks. In [78], adversaries manipulate IIoT localization systems by tampering with edge sensors, leading to untrustworthy positioning data. The proposed EM-based federated control framework iteratively verifies device trustworthiness through expectation–maximization (EM) algorithms. Additionally, reference [79] addresses edge server vulnerabilities by offloading sensitive computations to trusted cloud nodes using LDP and DRL-based task scheduling.

Despite these advances, challenges remain in scaling defenses across heterogeneous edge ecosystems. Reference [80] proposed a multi-center hierarchical FL (MCHFL) architecture that distributes aggregation tasks across edge servers, enhancing fault tolerance even when 50% of nodes are compromised. However, edge device heterogeneity complicates unified security enforcement, necessitating adaptive frameworks like SDN-based resource schedulers [81] that dynamically adjust communication protocols and encryption levels. Future directions include hardware-rooted security modules (e.g., TPM chips) and federated blockchain systems for immutable audit trails in edge networks.

3.4. Potential Solutions

3.4.1. Encrypted and Anonymized Privacy-Preserving Protocols

Reference [69] proposed the use of cloud–edge collaboration to deploy services in vehicular network scenarios dynamically and use HE to protect the uploaded model weights, reducing the risk of privacy leakage. At the same time, by collaborating with the cloud and edge to sink some services to the edge, it effectively reduces network communication overhead and meets low latency requirements. By encrypting the model weights before aggregation, HE can prevent adversaries from reconstructing the original data even if the transmission is intercepted.

In the metaverse environment, decentralized aggregation methods also require secure communication to ensure the reliability of multi-node collaboration. Reference [82] proposed the BFLMeta framework, which combines the blockchain and FL, capable of resisting single-point failures as well as preventing privacy leaks and poison attacks.

In response to the high security requirements of industrial edges, reference [83] presents a Blockchain-enhanced Grouped Federated Learning (BGFL) method, which improves security protection and robustness through local and global dual-layer aggregation and smart contract mechanisms; reference [84] proposed an HSADR scheme in Open Radio Access Networks (ORANs), which achieves IND-CCA2 level protection for secure aggregation by combining the consortium blockchain with DP.

Overall, utilizing secure protocols (e.g., TLS/VPN) coupled with the blockchain, HE, and comprehensive access control strategies can effectively ensure transmission security and model integrity in a cloud–edge–end collaborative environment. However, when applying these solutions in practice, it is crucial to fully consider issues like network jitter, terminal resource constraints, and node heterogeneity to ensure security while also focusing on performance and scalability.

Before the rise of FL, multi-hop privacy transmission, secret sharing, and multi-party secure computing (MPC) were also applied in distributed systems, attempting to reduce the trust risk in a single central node and weaken the threat of inference attacks through anonymization and noise injection. With the expansion of cloud–edge–end collaborative scenarios, these early schemes have gradually been integrated into the hierarchical FL system, providing diverse ideas for further enhancing data privacy protection.

Multi-hop privacy transmission reduces the chance of intermediate nodes leaking sensitive information by forming several "hops" or relays between edge nodes, distributing the flow of data or model updates. However, it is necessary to balance the relationship between the number of hops, latency, and cost. Secret sharing and anonymous protocols, using methods such as adding noise or secret splitting, divide sensitive data into several parts and cooperatively process it among multiple nodes, making it difficult to restore the complete original information even if a single point is attacked [72,85]. Combining DP and local perturbation technologies can further weaken the threat of the reverse inference to privacy.

Reference [72] applies the LDP strategy to add noise to the shared model parameters under the HFL framework, thereby preventing potential parameter analysis attacks during the upload process. This indicates that flexibly adjusting the privacy level in the cloud–edge–end multi-layer architecture can achieve DP protection while ensuring a certain level of model accuracy. Reference [85] points out that in Improved Multi-Layer Federated Learning (iMFL), to combat Data Reconstruction Attacks (DRAs), operations such as DP, sub-sampling, and gradient sign resetting are performed separately on end and edge devices after local training, effectively controlling communication overhead and privacy leakage risks. Reference [86] proposed a method for identifying abnormal or poisoned updates through Kalman filtering and Euclidean distance detection mechanisms at the edge side, in the application scenario of multi-level model aggregation from the cloud to the edge. This is a "layered fault tolerance" concept, beneficial for defending against external attacks and internal malicious nodes. In addition, reference [87] proposed a Multimodal Multi-Feature Construction (MMFFC) method at the feature level, which reduces the edge–cloud transmission volume by preprocessing data locally and reconstructing features while preserving privacy to a certain extent. This is a viable approach that parallels anonymization with performance improvement.

By comprehensively applying multi-hop privacy transmission, secret sharing, LDP, and anonymization techniques based on noise injection, the collaboration between the cloud, edge, and end can further reduce the dependence on central nodes and the potential risk of privacy leakage. However, in specific deployments, it is still necessary to consider how to balance the model's accuracy with the strength of privacy protection and to dynamically adjust according to network latency, bandwidth, and system throughput.

3.4.2. Deep Integration of FL and Trustworthy AI

In the multi-layered FL system of cloud–edge–end, relying solely on basic communication encryption or anonymization can cope with common risks such as data theft and network attacks, but it is still insufficient when facing poisoning attacks, systemic vulnerabilities, and higher-level trustworthy decision-making needs. To fundamentally enhance the robustness and traceability of the system, it is necessary to combine FL with trustworthy AI technology and construct a comprehensive security framework from multiple dimensions. Existing research has accumulated some experience in multi-layer model aggregation, heterogeneity management, and dynamic incentive mechanisms, laying the foundation for such integrated solutions.

Reference [88] enhances the model convergence speed by leveraging momentum acceleration (HierMo) in a three-level cloud–edge–end architecture and demonstrates an adjustable balance between aggregation cycles and transmission costs through theoretical analysis and experimental verification. Similarly, reference [89] achieves a balance between training efficiency and accuracy by adaptively adjusting the aggregation frequency and fully utilizing the heterogeneous features of node computing power. On this basis, ref-

erence [90] integrates personalized model training with the cloud–edge–end paradigm and more accurately captures local data features through learnable mixing parameters and normalization strategies, effectively addressing the differences in data distribution at the edge.

To further reduce the challenges brought by data heterogeneity and network overhead in distributed environments, some works have approached from the perspectives of group management and incentive mechanisms. When facing massive edge nodes, rational group management can effectively reduce the communication burden and the impact of heterogeneity during model aggregation. Reference [91] indicates that reasonable grouping helps alleviate the negative impact of heterogeneity among nodes on convergence performance. In response to long-term imbalanced data distribution and inconsistent node participation, reference [92] introduces a method combining Age of Update (AoU) with reputation and data volume to avoid over-reliance on the same batch of devices and promote global model convergence more fairly and efficiently.

However, relying solely on the optimizations and improvements made at the FL level cannot completely address the deeper security risks, such as adversarial attacks, decision explainability, and auditability. As the scale of cloud–edge–end collaboration continues to expand and the complexity of application scenarios increases, achieving multi-party trustworthy, verifiable, and scalable AI systems becomes an inevitable trend.

Existing solutions to privacy and security challenges are gradually evolving from isolated techniques toward integrated frameworks that combine encryption, access control, anonymization, and trustworthy AI. In future systems, these elements must work in synergy to support secure, adaptive, and scalable cloud–edge–end federated architectures.

4. FL Meets Trusted AI

4.1. Foundations of FL

4.1.1. Overview of FL

FL has emerged as a promising paradigm for distributed and privacy-preserving AI collaboration. It allows for the training of AI models with massive devices at the edge while protecting user privacy. In traditional federal learning, devices train local models with their private data and submit model parameters rather than raw data to the parameter server [3]. Hierarchical federal learning optimizes the communication efficiency and scalability of traditional federal learning by introducing edge computing nodes (base stations and edge servers) as intermediate aggregation layers [88,89]. Google's FedAvg [3] can be extended to HierFAVG [93], which aggregates some device parameters at the edge layer before uploading them to the cloud, and its edge layer can operate independently, with local failures not affecting the global system. Figure 3 shows the architecture of traditional federal learning and hierarchical federal learning.

In different FL application scenarios, there are differences in the features of the datasets collected between clients. Depending on the distribution patterns of the data sample space and feature space, FL can be categorized into Horizontal Federated Learning (HFL), Vertical Federated Learning (VFL), and Federated Transfer Learning (FTL). This is illustrated in Figure 4.

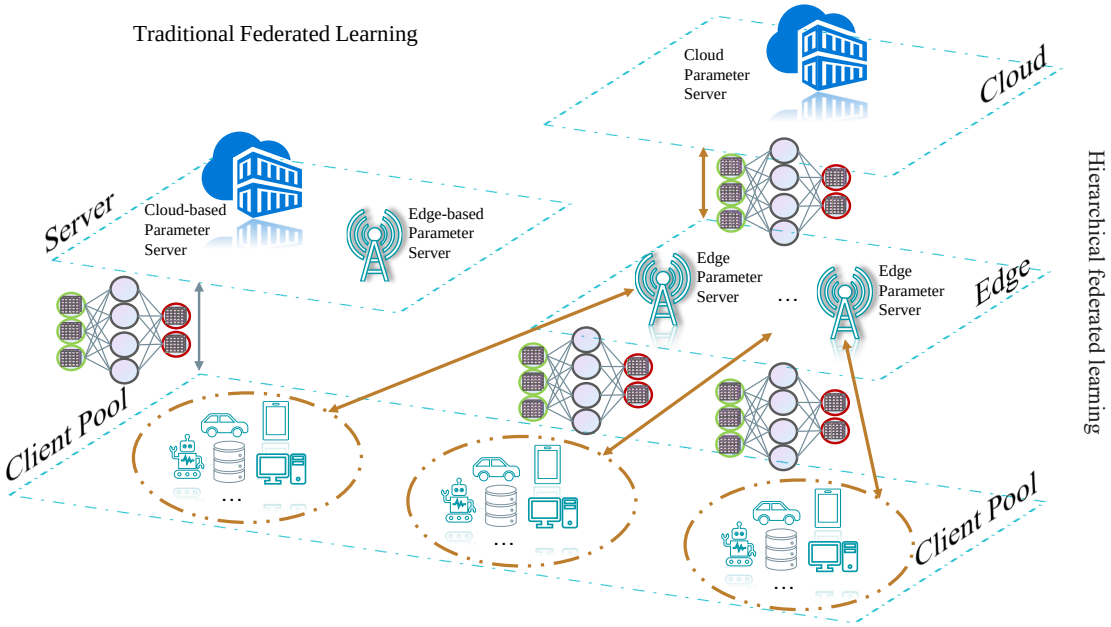

Figure 3. The architecture of traditional federal learning and hierarchical federal learning.

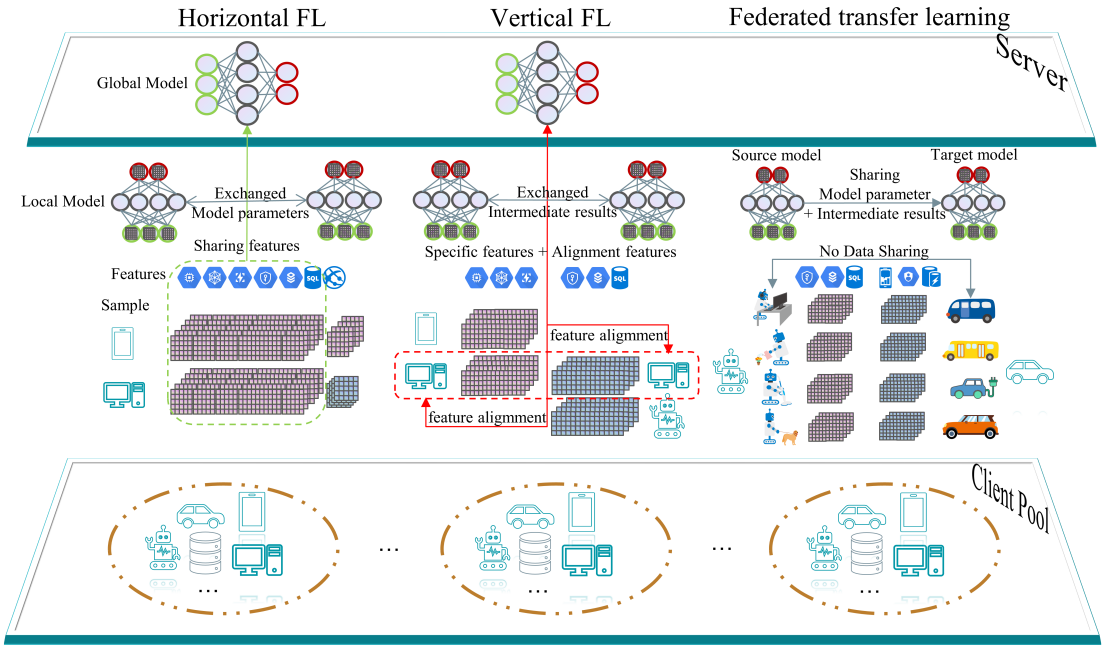

Figure 4. Classification of FL.

4.1.2. Horizontal FL

HFL is applicable to scenarios where the feature space of the participating parties' data is the same, but the sample space is different (i.e., "same features, different samples"), that is, each client has its own dataset and trains the model parameters independently. The centralized aggregation of model parameters enables collaborative learning across parties without sharing raw data. Typical applications include collaborative model training across devices (e.g., mobile input method prediction) and the collaboration of same-domain data across institutions (e.g., multiple hospitals jointly training disease diagnosis models).

A widely adopted mathematical formulation was proposed by McMahan et al. in the seminal FedAvg algorithm [3]. The goal is to minimize a global objective function composed of local empirical losses:

$$\min_{\omega \in \mathbb{R}^d} f(\omega) = \sum_{k=1}^{K} \frac{n_k}{n} F_k(\omega), \quad \text{where} \quad F_k(\omega) = \frac{1}{n_k} \sum_{i \in \mathcal{P}_k} \ell(x_i, y_i; \omega). \tag{1}$$

Each selected client k performs local updates (e.g., using SGD) on its data and returns the locally trained model ω_k^{t+1} to the server. The server then performs weighted aggregation to update the global model:

$$\omega_{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} \omega_k^{t+1}. \tag{2}$$

This formulation captures the key traits of HFL, such as non-IID local data, communication constraints, and decentralized optimization. It has inspired a wide range of subsequent FL variants, as shown below:

- Privacy protection methods in HFL
  To solve the problem of data security and confidentiality in the distributed data environment in pattern recognition, reference [94] proposed a classifier based on fuzzy rules. Reference [95] studied the reliability of participants, integrity, and credibility of messages in the medical IoT and proposed a privacy-preserving disease research system based on HFL. Reference [96] focused on the automatic detection of IoT devices and proposed a HFL scheme HFedDI, which is scalable and can improve the performance of device recognition in various scenarios. Reference [97] designed a novel FL architecture named EHFL, which protects data privacy by using single masking and group key encryption and significantly reduces the computation and communication overhead of clients.
- Applications in HFL
  In a smart grid, reference [98] proposed a dynamic security assessment method EFed-DSA for a smart grid based on HFL and DP, which combines a Gaussian mechanism to protect the privacy of distributed dynamic security assessment (DSA) operation data. And in order to improve the operational safety and reliability of a distribution network, reference [99] proposed a new deep learning method to estimate the baseline load (CBL) of residential loads while applying HFL to local neural network training in residential units to protect the privacy of residential customers. Aimed at the data feature selection in the IoT, reference [100] proposed an unsupervised joint feature launch selection method, FSHFL, based on HFL, which can select a better federated feature set among participants in HFL to improve system performance. In addition, with respect to network dynamic programming technology, improving the operational safety and reliability of a distribution network, reference [101] used FL to model virtual network embedding (VNE) for the first time and proposed a VNE architecture, HFL-VNE, based on HFL, which can dynamically adjust and optimize the resource allocation of multi-domain physical networks.

4.1.3. Vertical FL

VFL targets scenarios where the participating parties share the same sample space but different feature spaces (i.e., "same samples, different features"). Typical use cases include cross-industry data fusion (e.g., joint risk control modeling by banks and e-commerce) and crossmodal feature complementarity (e.g., collaborative analysis of medical imaging and genomic data). Compared to HFL, where model parameters are averaged across clients,

VFL requires a more sophisticated protocol to securely compute collaborative updates across distributed features.

A representative implementation is SecureBoost [102], a federated gradient tree boosting framework that constructs decision trees across parties without exposing private data. In this setting, the model prediction at iteration t is incrementally constructed through additive trees:

$$\hat{y}_i = \sum_{k=1}^{K} f_k(x_i). \tag{3}$$

To select the optimal split during tree construction, the split gain is computed as

$$\mathcal{L}_{\text{split}} = \frac{1}{2}\left(\frac{G_L^2}{H_L+\lambda} + \frac{G_R^2}{H_R+\lambda} - \frac{(G_L+G_R)^2}{H_L+H_R+\lambda}\right) - \gamma. \tag{4}$$

Here, G_L and H_L (resp., G_R and H_R) represent the sums of first-order and second-order gradients for samples in the left (resp., right) child node. Once the optimal split is found, the weight of leaf node j is computed as

$$w_j^* = -\frac{G_j}{H_j+\lambda}, \quad \text{where} \quad G_j = \sum_{i\in I_j} g_i, H_j = \sum_{i\in I_j} h_i, g_i = \frac{\partial l(y_i,\hat{y}_i)}{\partial \hat{y}_i}, h_i = \frac{\partial^2 l(y_i,\hat{y}_i)}{\partial \hat{y}_i^2}. \tag{5}$$

To protect privacy, the gradients g_i and h_i are encrypted using an additive homomorphic encryption scheme before being shared between parties. Passive parties compute encrypted candidate splits locally and send the encrypted statistics back to the active party, which decrypts them to determine the global optimal split. Throughout this process, no raw features or labels are exchanged. The privacy protection methods, attack and defense strategies, model training efficiency, and applications in VFL are as follows:

- Privacy protection methods in VFL
  Reference [103] proposed an adaptive DP protocol for FL, AdaVFL. This protocol estimates the impact of organizations' features on the global model and designs two weighting strategies to allocate the privacy budget adaptively for each organization, protecting its features heterogeneously. Reference [104] introduces a new protocol based on XGBoost called FEVERLESS, which utilizes information masking techniques and global differential privacy to prevent the leakage of private information during training. Reference [105] presents a new method for obtaining encrypted training datasets, termed NCLPSI, for privacy protection in VHL. Furthermore, reference [106] explores an efficient and privacy-preserving VFL framework based on the XGBlust algorithm, ELXGB. To address the slow convergence rate of VFL based on zero-order optimization when dealing with large modern models, a cascaded hybrid optimization method is proposed [107].
- Attack and defense strategies in VFL
  VFL faces several security threats, including backdoor attacks and label inference attacks. In VFL, the backdoor attack is a serious threat, where the attacker manipulates the model's predictions by injecting specific triggers into the training dataset. Reference [108] proposed a novel and practical method (BadVFL), which enables the injection of backdoor triggers into the victim model without label information. Reference [109] explores the vulnerability of VFL in binary classification tasks and introduces a universal adversarial backdoor attack to poison VFL's predictions. Reference [110] addressed the vulnerability of data protection during the VFL training phase and proposed a novel defense mechanism to obfuscate the association between bottom model changes and labels (i.e., features) during training. Also, for label in-

ference attacks in VFL, where attackers speculate on other participants' labels based on the trained model, leading to serious privacy leaks, reference [111] proposed a threshold filtering-based detection method and created six threat model categories based on adversary prior conditions.

- Model training efficiency in VFL
  In order to improve the efficiency and performance of VFL, addressing the issues of synchronous computation and HE in VFL, reference [112] proposed an efficient asynchronous multi-party vertical federated learning method (AMVFL), significantly reducing the computational function cost and enhancing the accuracy of the model. Meanwhile, reference [113] analyzed the bottlenecks of VFL under HE and proposed a system that is resistant to procrastination and is computationally efficient for acceleration. Reference [114] introduces a novel communication-efficient VFL algorithm named FedONce, which only requires a single communication between parties, greatly improving the communication efficiency of VFL.
- Applications in VFL
  VFL provides convenience for cross-domain data collaboration, but it still faces challenges such as uneven data distribution, inconsistent features, and high communication costs. Due to the varied imaging guidelines of different hospitals, resulting in data with the same modality being difficult to meet the needs of practical applications, reference [115] proposed a Federated Consistent Regularization Constrained Feature Disentanglement (Fed-CRFD) framework for how to perform collaborative learning while maintaining privacy between multiple hospitals. This framework enhances MRI reconstruction by effectively utilizing overlapping samples (i.e., the same patient with different modalities in different hospitals) and solving the domain shift caused by different modalities. Another study focuses on wireless traffic prediction, emphasizing the issues of traditional centralized training methods in terms of data transmission, latency, and user privacy [116]. For this reason, reference [116] introduced a wireless traffic prediction framework based on partition learning and VFL. This framework enables multiple edge clients to collaboratively train high-quality prediction models by leveraging diverse traffic data while keeping the raw data confidential locally. Reference [117] conducted research on fine-grained data distribution in real-world FL applications. They proposed a VFL framework, HeteroVFL, to address the complexity of data distribution, and enhanced the privacy of HeteroVFL by adopting DP.

4.1.4. Federated Transfer Learning

FTL, as a deep integration paradigm of FL and transfer learning (TL), aims to address the contradiction between data heterogeneity and privacy protection in distributed multi-party scenarios. Unlike traditional FL, FTL not only needs to tackle the non-IID issues related to feature space ($X_i \neq X_j$), label space ($Y_i \neq Y_j$), or joint probability distribution ($P(X_i, Y_i) \neq P(X_j, Y_j)$) but also has to overcome the risks of system heterogeneity ($F_i \neq F_j$) and the scarcity of global labeled data ($X_L \to 0$) leading to model degradation. By designing cross-domain knowledge transfer mechanisms, combined with parameter sharing, feature alignment, and distributed aggregation strategies, it achieves an implicit mapping of local knowledge to global representations, thereby enhancing the model's generalization capability without the need for data centralization. A widely adopted FTL framework jointly optimizes the following loss [118]:

$$\min_{\theta^A, \theta^B} \mathcal{J} = \mathcal{L}_{pred} + \beta \mathcal{L}_{align} + \alpha \left(\left\| \theta^A \right\|^2 + \left\| \theta^B \right\|^2 \right). \tag{6}$$

Here, $\mathcal{L}_{pred}$ represents the supervised loss over available labels, $\mathcal{L}_{align}$ is a latent representation alignment loss over common samples, and the final term penalizes model complexity. α and β are the weight parameters. Specifically, the label prediction loss can be instantiated as

$$\mathcal{L}_{pred} = \frac{1}{|\mathcal{C}|} \sum_{i \in \mathcal{C}} \ell(y_i, \phi(h_i^B)), \quad \phi(h_i^B) = \sum_{k \in \mathcal{A}} \omega_k (h_k^A \cdot h_i^B), \tag{7}$$

where h_k^A and h_i^B are the embedded features from parties A and B, and $\phi(\cdot)$ approximates cross-party prediction via similarity fusion.

To protect data privacy during collaborative training, a second-order Taylor approximation is employed for secure gradient computation:

$$\ell(y, \phi) \approx \ell(y, 0) + \kappa_1(y)\phi + \kappa_2(y)\phi^2. \tag{8}$$

with a corresponding gradient as follows:

$$\frac{\partial \ell}{\partial \phi} = \kappa_1(y) + 2\kappa_2(y)\phi. \tag{9}$$

This framework enables secure, collaborative model training across heterogeneous and isolated data domains by aligning intermediate features and applying privacy-preserving optimization techniques. FTL knowledge transfer and applications are discussed below:

- Knowledge transfer in FTL
  Due to the heterogeneity and distribution discrepancy of data, how to effectively transfer knowledge is a key problem. Reference [119] proposed the knowledge transfer method called PrivateKT, which transfers high-quality knowledge using actively selected small public data with privacy-preserving FL. Reference [120] defined FTL without labels in the source domain, conducted research on the road crack benchmark, and proposed a fedCrack model that obtains a pretrained encoder on the source domain without accessing the annotations. Reference [121] proposed a joint knowledge transfer (FedKT) method for the deficiencies of model learning caused by heterogeneous data distribution in the process of model collaborative training, which utilizes the advantages of fine-tuning and knowledge distillation to effectively extract general knowledge and specific knowledge from the early layers and output of the global model, respectively, so as to improve the learning performance of the local model. Reference [122] proposed federated fuzzy transfer learning (FdFTL) for class transformation, which can be trained across domains without data sharing. In order to overcome the data heterogeneity problem, reference [123] proposed a FedKT framework, which takes into account both diversity and consistency among clients and can serve as a general solution for knowledge extraction from distributed nodes. Reference [124] proposed a device selection method based on multi-objective optimization (MOO) and knowledge transfer (KT) for heterogeneous FL systems, so as to alleviate resource constraints while improving accuracy.
- Applications in FTL
  In order to realize cross-domain fault diagnosis without data sharing, reference [125] proposed a fault diagnosis model based on Federated Transfer Learning. Reference [126] put forward a completely decentralized Federated Transfer Learning fault diagnosis method to solve the privacy and domain shift problems in deep learning. In response to the challenges of electricity load estimation caused by global population growth and the increasing demand for intelligent devices, reference [127] combines clustering analysis with joint transfer learning to construct a household-level prediction model.

Reference [128] proposed a privacy protection framework for heating, ventilation, and air conditioning (HVAC) systems in buildings, which combines FL and transfer learning to evaluate the adjustment ability of HVAC systems. Reference [129] presents a collaborative learning framework for IDSs used in IoMT applications, which can achieve a detection accuracy of up to 95–99%.

The above works all highlight the importance of ensuring data privacy and security in practical engineering applications and propose specific methods and techniques for different application fields and problems.

A comparative summary of the key mathematical formulations used in HFL, VFL, and FTL is provided in Table 1, illustrating the respective objectives, computation targets, and privacy-preserving mechanisms.

Table 1. Summary of typical mathematical formulations in federated learning paradigms.

FL Type	Objective/Formulation	Key Variables	Privacy Mechanism
HFL	Global loss minimization: $\min_{\omega} \sum_{k=1}^{K} \frac{n_k}{n} F_k(\omega)$ Global model update: $\omega^{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} \omega_k^{t+1}$	Local losses F_k, model ω	Only model parameters shared
VFL	Split gain: $\mathcal{L}_{\text{split}} = \cdots$ (Equation (4)) Leaf weight: $w_j^* = -\frac{G_j}{H_j+\lambda}$ (Equation (5))	Gradients g_i, h_i	Encrypted statistics, no label sharing
FTL	Joint loss: $J = L_{\text{pred}} + \beta L_{\text{align}} + \alpha(\|\theta^A\|^2 + \|\theta^B\|^2)$ Prediction loss: $L_{\text{pred}} = \sum \ell(y, \varphi(h_i^B))$	Cross-party embeddings, θ^A, θ^B, φ	Feature alignment, secure approximation

In summary, HFL, VFL, and FTL reflect three paradigms of adapting FL to data heterogeneity and application needs. These paradigms differ in the alignment of feature and sample spaces, but all share a common goal of enabling collaborative intelligence while preserving privacy. This taxonomy also lays the groundwork for matching trust, robustness, and resource strategies in Section 4.2.

4.2. Pillars of Trustworthy AI in Federated Context

4.2.1. Dimension Reconstruction of Trusted AI

The trustworthiness requirements of traditional AI, represented by the EU's ALTAI framework, focus on seven core principles, including technical robustness, fairness, and transparency. However, the distributed characteristics of FL (data isolation and heterogeneity of participants) pose new challenges to trustworthiness:

- Data Isolation: The privacy protection of traditional AI needs to be extended to collaborative training across clients, but data invisibility hinders global data quality verification and attack detection.
- Participating Heterogeneity: Device heterogeneity and non-IID data across clients challenge traditional indicators (e.g., global fairness). In medical FL, the differences in data distribution between hospitals may mask biases against minority groups, while the low computing power of edge devices limits the deployment of complex robustness algorithms.

To address the above challenges, the trustworthiness of FL needs to be reconstructed as a three-dimensional collaborative framework:

- Data Trustworthiness
  Data trustworthiness ensures the authenticity, representativeness, and security of local data on the client side, preventing low-quality or malicious data from contaminating

the global model and providing a reliable input for subsequent training. However, under data isolation, it is impossible to directly detect malicious samples (e.g., adversarial samples or poisoned data). In response to this, adversarial detection models are trained through federated collaboration, using local validation sets on the client side to identify abnormal data patterns. It is also possible to record statistical characteristics of data (e.g., mean and variance) based on the blockchain and exclude outlier clients through a consensus mechanism [130], achieving a consensus on data quality.

- Process Trustworthiness
  Process trustworthiness focuses on two key goals: ensuring fairness and enabling traceability during the aggregation process. It prevents a few parties with dominant resources or data from monopolizing model evolution, thereby enhancing overall fairness. However, the participation of heterogeneous clients may lead to biases in contribution evaluations, such as clients with high data volumes dominating model updates. To address this, the Bayesian decision rules and evidence theory can be employed to quantify the uncertainty and performance of each client, providing a reliable strategy for client selection [131]. Additionally, malicious clients can be identified and suppressed through gradient similarity analysis or rule activation tracking [132].
- Outcome Trustworthiness
  Outcome trustworthiness ensures that global model decisions are transparent and consistent with domain knowledge, providing consistent decision explanations for cross-domain participants and supporting the implementation of models in high-trust scenarios such as clinical and industrial settings. However, data isolation leads to the inability of traditional explainable methods to generalize local explanations. To address this, it is important to extend Shapley values to federated scenarios [130], calculating global feature importance through encrypted gradient aggregation. At the same time, it is important to sparsify model parameters that are unrelated to decisions and retain causal association paths [133] to build a causally explainable framework.

The aforementioned three dimensions are not isolated but achieve trust enhancement through technological linkage: Data→Process: high-quality data input improves the accuracy of a contribution assessment [132]. Process→Results: fair aggregation reduces model bias, thereby improving explanatory consistency [134]. Results→Data: global explanations feedback to enhance data quality verification [135].

4.2.2. The Foundation of the Trustworthiness Pillar

Robustness

The robustness of FL requires the system to maintain model performance stability and functional integrity in the face of malicious attacks, data noise, or device failures. Unlike traditional centralized AI, the robustness in federated scenarios needs to address the openness of a decentralized architecture, the heterogeneity of data/devices (non-IID), and the feasibility of defense under resource constraints [3,33,34]. For instance, while the FedAvg algorithm proposed by McMahan et al. lays a foundation for privacy protection, its default aggregation mechanism lacks defense capabilities against Byzantine attacks, and the dynamism of devices in edge computing scenarios (e.g., going offline and computational power fluctuations) further exacerbates the difficulty of ensuring robustness [33,136].

The open-architecture nature of FL introduces a multi-dimensional attack surface, and the main threats include the following:

- Byzantine Attacks
  Malicious clients upload tampered gradients (e.g., gradient reversal and random noise) to disrupt the convergence of the global model. Although the Krum algorithm [137]

can filter explicit abnormal gradients, it relies on statistical properties of gradients and is difficult to defend against covert poisoning attacks [137,138].

- Gradient Poisoning
  The model is made to fail under certain trigger conditions by Backdoor Injection [138].
- Data/Device Unreliability
  Failures of edge devices [139] or data noise [140] can lead to model performance degradation. Reference [140] points out that traditional federated algorithms generally do not detect data noise, resulting in reduced model robustness.

Table 2 compares the core technical directions and their innovative points in robustness enhancement in FL. To address the above threats, researchers propose multi-level defense strategies:

Table 2. Comparison of key technologies for robustness enhancement in FL.

Research Direction	References	Main Findings	Research Significance
Robust Aggregation and Dynamic Topology Optimization	[33,141]	Ref. [33]: hierarchical aggregation clusters edge nodes to reduce communication overhead and limit the impact of malicious nodes; Ref. [141]: the CoCo algorithm adaptively constructs P2P topology, and the consensus distance measurement accelerates convergence (10 times speed improvement).	It optimizes communication efficiency and anti-attack capabilities of a decentralized architecture, suitable for the IIoT and dynamic network environments.
Byzantine Attack Defense Algorithm	[137]	Ref. [137]: the Krum algorithm filters explicit anomalies through gradient statistics, and is the first provably Byzantine-robust aggregation rule.	It provides theoretical guarantees for open federation scenarios and resists explicit attacks such as gradient inversion and noise injection.
Privacy Enhancement and Blockchain Auditing	[142,143]	Ref. [142]: the chain-PPFL framework combines chain-style secure multi-party computation with DP ($\epsilon \rightarrow 0$); Ref. [143]: the blockchain records model signatures, tracing malicious client poisoning behavior.	While protecting gradient privacy, it enhances model traceability, supporting trustworthy collaboration in smart home and energy scenarios.
Resource-Aware Defense Mechanism	[144,145]	Ref. [144]: the EAFL scheme offloads computation from slow devices to the edge, reducing the poisoning window; Ref. [145]: the FedMP framework dynamically prunes to adapt to heterogeneous device resources, achieving an acceleration of 4.1 times.	It alleviates the contradiction between defense feasibility under resource constraints, balancing the efficiency and security of edge computing.
Attack Detection and Anomaly Filtering	[138,140]	Ref. [138]: Standardized DP and norm truncation resist backdoor attacks; Ref. [140]: the RoFed method filters noisy devices through the angle of the gradient direction.	It enhances the model's robustness against covert poisoning attacks and data noise, ensuring reliable decisions in medical and power scenarios.

- Robust Aggregation Algorithm
  - Hierarchical Aggregation: Reference [33] proposed the resource-efficient FL with hierarchical aggregation (RFL-HA), which reduces communication overhead and limits the impact of malicious nodes through edge node clustering, but it may introduce the risk of a single point of failure within the cluster.
  - Dynamic Topology Optimization: The CoCo algorithm [141] adaptively constructs P2P topology and compresses model parameters, accelerating convergence under non-IID data (10 times speedup), but its consensus distance measure may fail in extremely heterogeneous scenarios.
- Privacy-Enhancing Defense
  - DP: The chain-PPFL [142] combined chain-secure multi-party computation with LDP to achieve gradient privacy protection ($\epsilon \to 0$), but excessive noise injection may weaken the robustness of the model [146].
  - Blockchain Auditing: Reference [143] leveraged decentralized ledgers to record contributions and detect tampering. In the smart home scenario, the blockchain traces model signatures of malicious clients while preventing poisoning attacks. However, its integration may also introduce latency from consensus protocols and additional storage/computation overhead, especially in edge-based federated deployments.
- Resource-Aware Defense
  - Adaptive Pruning: The FedMP framework [145] dynamically adjusts the pruning rate through a MAB to achieve efficient defense on resource-constrained devices, but its residual recovery synchronization (R2SP) mechanism is sensitive to non-IID data.
  - Edge-Assisted Computation: The EAFL scheme [144] offloads the computation tasks of stragglers to edge servers, reducing the window of poison attacks, but it is necessary to optimize the amount of offloaded data to balance efficiency and security.

Furthermore, the robustness of the federation needs to be quantified through multi-dimensional indicators:

- Adversarial Sample Detection Rate
  The RoFed method [140] filters the abnormal devices through the gradient direction angle to prevent the end devices trained with noisy data from participating in the parameter aggregation on the cloud device.
- Model Accuracy Fluctuation Threshold
  The FedSens framework [38] combines RL and an adaptive updating strategy in abnormal health detection (AHD), which makes the F1-score exhibit lower fluctuations to handle class imbalance data, ensuring performance stability across multiple iterations and different devices.
- Resource Efficiency Metrics
  - Communication Overhead: The edge clustering scheme of paper [147] reduces the amount of transmissions of local updates by 60%.
  - Computation Latency: The EAFL framework [144] reduces the system delay.

The cross-scenario experiments verify the effectiveness of the defense mechanism. In the medical field, CFL improves the F1-score by 16% in the diagnosis of COVID-19 medical images while resisting data noise [53]. In the IIoT, the AMCNN-LSTM model [139] combined with gradient compression reduces communication overhead by 50% in sensor

anomaly detection. The AAFL framework [148] dynamically adjusts the aggregation ratio α through DRL, reducing the training completion time by 70%.

Although the existing technologies significantly promote the fed robustness, there are disputes and challenges that still need to be resolved as follows:

- Privacy–Robustness Paradox
  PoisonGAN [146] attacks demonstrate that DP noise may weaken the model's ability to detect poisoning attacks (the lower the privacy budget ϵ, the higher the backdoor success rate). Comparing chain-PPFL [142] and the PFLF framework [149], there is an inherent trade-off between LDP and model convergence speed (while PFLF reduces communication overhead through flexible participation mechanisms, it requires sacrificing some privacy strength).
- Fairness–Robustness Conflict
  The FedSens framework [38] reveals that excessive emphasis on robustness (e.g., strict client selection) under the medical data imbalance scenario may exacerbate model bias.
- Adaptability to Dynamic Environments
  The existing CoCo scheme [141] relies on the assumption of a static network, which is difficult to cope with extreme dynamic scenarios (e.g., the dramatic changes in topology in drone swarm federations [150]).

Future research needs to focus on three main directions: lightweight robust aggregation (combining pruning with dynamic topology optimization), attack–defense game modeling (utilizing RL to dynamically adjust strategies), and cross-layer trustworthy collaboration (deeply integrating edge computing with blockchain technology). Through multi-dimensional innovation, FL can achieve the co-evolution of privacy, efficiency, and robustness in an open environment.

Fairness

Fairness in FL aims to ensure that all participating clients (especially edge devices) are treated equally during model training, avoiding systematic neglect or the discrimination of specific groups due to data distribution, resource differences, or participation mechanisms. This goal faces unique challenges in federated scenarios: data heterogeneity (non-IID) may amplify group biases, client dynamics (e.g., frequent device dropouts) exacerbate participation imbalances, and resource constraints (e.g., computational and energy limitations) force the system to trade between efficiency and fairness [151–153]. Zhang et al. [153] pointed out that the decentralized nature of FL may lead to a "fairness paradox"—prioritizing high-resource clients (e.g., high-performance nodes in Vehicle Edge Computing [151]) to improve the global model performance ironically leads to the systematic exclusion of edge devices, further aggravating data biases [153]. This contradiction is particularly prominent in real-world scenarios such as smart grids [154] and medical edge computing [38], where the local data of low-resource clients might represent minority groups or special cases. Their absence will reduce the model's generalization capability or result in suboptimal models.

Table 3 compares the core technical directions and innovative points of fairness enhancement in FL. To address the above challenges, researchers have proposed solutions from two dimensions, client selection and loss function design:

Table 3. Comparison of key technologies for fairness enhancement in FL.

Research Direction	References	Main Findings	Research Significance
Dynamic Resource Allocation and Client Selection	[151,152,155]	Ref. [151]: dynamically selects high-contribution vehicles based on image quality, jointly optimizing computation, transmission, and model accuracy; Ref. [155]: matching the game allocation task, reducing the participation imbalance of high-mobility devices.	Enhancing the fairness of participation in Vehicle Edge Computing (VEC) and IoT scenarios, optimizing the resource utilization rate and model performance.
Blockchain-Driven Trustworthy Incentive Mechanism	[156–158]	Ref. [156]: the two-layer blockchain records the reputation, and the smart contract rewards high contribution devices; Ref. [158]: the InFEDge framework combines multi-agent game theory with contract theory to solve the problem of information asymmetry.	It enhances the fairness and transparency of device participation, suppresses malicious nodes, and supports credible collaboration in edge computing scenarios.
Heterogeneous Client Adaptation and Migration Learning	[153,159,160]	Ref. [159]: FTL constructs multiple global models to adapt to clients with different resource levels; Ref. [160]: DRL adaptively adjusts the integrated air-space-ground task offloading strategy.	This alleviates the participation bias caused by resource heterogeneity, ensuring fair opportunities for low-power devices in dynamic environments.
Federal Fairness Loss Function Design	[154,161]	Ref. [154]: multi-objective optimization and dynamic adjustment of loss weights with DRL, incentivizing high-quality model sharing; Ref. [161]: agnostic FL minimizes the upper bound of the worst client loss.	It addresses group bias caused by non-IID data, enhancing model generalization in medical and energy scenarios.
Privacy–Fairness Collaborative Optimization	[162,163]	Ref. [162]: PFCEL quantifies the trade-off between leakage risk and model accuracy through the Stackelberg game; Ref. [163]: the blockchain trusted computing framework realizes data are “usable but invisible”.	While protecting the privacy of sensitive data, it ensures the fairness of participation, promoting compliant AI applications in the fields of smart grids and healthcare.

- Client Selection Strategies
  - Dynamic Selection and Resource Awareness: In VEC, reference [151] proposed a greedy algorithm based on image quality, dynamically selecting high-contribution vehicles to participate in training, while jointly optimizing computational capability, transmission power, and model accuracy to minimize the overall system cost. Similarly, reference [155] allocates tasks in Multi-access Edge Computing (MEC) through matching game theory, reducing the uneven participation time of

large-scale IoT devices caused by high mobility, thereby improving task allocation fairness while reducing latency.

- Incentive Mechanism and Trustworthy Evaluation: The introduction of blockchain technology provides new ideas for fair participation. Reference [156] designs a two-layer blockchain architecture (LMUC and GMUC), which records the historical reputation of local model updates through D2D communication, and combines smart contracts to reward devices with high reputation, suppressing the influence of malicious nodes. The InFEDge framework proposed [157] further models the incentive mechanism as a multi-agent Stackelberg game, using contract theory to solve the problem of information asymmetry, ensuring that resource-constrained devices obtain reasonable compensation when contributing data. In addition, reference [164] proposed a reputation-based node selection algorithm (NSRA), which predicts device reputation in HFL, prioritizes the selection of devices with a high reputation to participate in training, and enhances the collaborative trust between devices through D2D communication, improving the model accuracy by 11.48% and 19.38% in MNIST and CIFAR-10 tasks, respectively.

- Loss Function Reconstruction and Heterogeneous Processing
  - Federated Fairness Loss Function: The Agnostic FL framework [161] alleviates group bias caused by data heterogeneity by introducing a fairness constraint term to minimize the upper bound of the worst client's loss. This idea is further extended in the smart grid scenario. Reference [154] combined local data evaluation mechanisms, designed multi-objective optimization problems, and used DRL to dynamically adjust the weights of the loss function, incentivizing Energy Data Owners (EDOs) to share high-quality model updates.
  - Heterogeneous Client Adaptation: Addressing the heterogeneity of device resources and model architectures, reference [159] proposed an FTL framework, constructing multiple global models to adapt to clients with different resource levels. In the CIFAR-100 task, the training time for clients with abundant resources is significantly lower than that for constrained devices, and through grouped training and transfer learning, the overall convergence time is shortened. Similarly, reference [160] adopted DRL in air-space-ground integrated edge computing to adaptively adjust the task offloading strategy, balancing energy efficiency and computational fairness, ensuring the participation opportunities for low-power IoT devices in uncertain communication environments. Reference [153] focuses on the AI-driven healthcare sector, proposing a resource-adaptive framework for collaborative learning, which can dynamically adapt to varying computational capabilities to ensure fair participation.

Furthermore, fairness needs to be quantified through multi-dimensional indicators, and the effectiveness of the technology should be verified in cross-scenario experiments:

- Performance Differences Across Clients
  The Fedsens framework [38] in the anomaly detection of medical data exhibits lower fluctuations when dealing with class-imbalanced data. The blockchained dual-asynchronous federated learning framework (BAFL-DT) [158] achieves global model aggregation through DT technology, statistically analyzing the standard deviation of accuracy across clients during asynchronous training, verifying its fairness advantages under non-IID data.
- Contribution Assessment and Incentive Mechanism
  Shapley values are widely used to quantify the contribution of clients, but their computational complexity limits their application in large-scale scenarios. Reference [165]

models the incentive distribution in hierarchical FL through the Stackelberg game, derives the Nash equilibrium strategy, and proves that it can reduce participation costs while increasing model convergence speed in high dynamic edge cloud scenarios.

- Privacy–Fairness Trade-off
  Reference [162] designed a privacy protection incentive mechanism in federated cloud–edge learning (PFCEL), quantifying the relationship between data leakage risk and model accuracy through a three-level Stackelberg game. Experiments show that this mechanism, while protecting the privacy of sensitive devices, enhances system utility, verifying the synergistic feasibility of privacy and fairness. The resource-adaptive framework [153] improves model accuracy, safeguards patient privacy, and promotes equitable access to trustworthy and efficient AI-driven healthcare solutions.

Despite remarkable technological advances, federal fairness remains a core controversy:

- The Persistence of Fairness Paradox
  Although existing mechanisms (e.g., dynamic selection and incentive mechanisms) can alleviate participation imbalance to a certain extent, they cannot completely eliminate the bias caused by data heterogeneity. In smart grids, high-resource devices may still dominate model updates, leading to the neglect of the electricity consumption patterns of edge household users [154]. Therefore, in the FL paradigm, it is necessary to design methods that are more sensitive to resources [153].
- Limitations of Evaluation Metrics
  In federated scenarios, the contribution of clients with high data volume may be overestimated, while the weight of low-resource but high-value data may be underestimated. Although incentive mechanisms can encourage client participation [165], they are constrained by their own computational resources and cannot join. Moreover, the blockchain trusted computing framework [163] can enhance the transparency of data interaction, but its public ledger may leak the device participation pattern, thus harming fairness.
- Adaptability to Dynamic Environments
  Existing methods (e.g., DRL offloading strategy [160]) largely rely on static network assumptions, making it difficult to cope with extreme dynamic scenarios (e.g., dramatic topology changes in drone swarms). Moreover, the delay in blockchain consensus [157,158] may intensify resource competition and reduce the enthusiasm of participation from devices with low computational power.

We can observe that research on the fairness of FL is evolving from single algorithm optimization to multi-dimensional system design, covering aspects such as dynamic resource allocation, trustworthy incentive mechanisms, and heterogeneous model adaptation. However, the combined effects of data heterogeneity, device dynamism, and privacy constraints remain core challenges. In the future, through interdisciplinary integration (e.g., game theory, the blockchain, and RL), it is necessary to build a trustworthy federated architecture that takes into account efficiency, privacy, and fairness. Only then can truly inclusive AI empowerment be realized in key scenarios such as smart grids, vehicular networks, and medical edge computing.

Explainability

The explainability of FL requires the model decision logic to be transparent to participants while ensuring cross-client data privacy. This goal faces a dual dilemma in the federated scenario: model black-boxiness and data isolation. Traditional explainability methods (e.g., LIME [166] and Shapley values [167]) rely on global data feature analysis, but the data localization characteristics of FL cause the absence of a global feature view, resulting in fragmented and credibility-challenged explanation results. In the medical field,

federated models involving multi-institutional collaboration need to explain the contributions of multimodal data (e.g., MRI and clinical indicators [134]) to disease prediction, but data isolation makes it difficult for local explanation at a single client to reflect the global decision logic [133]. Moreover, privacy protection mechanisms may perturb key model parameters, further blurring the explanation path [168].

The special challenges of explainability in federated scenarios include the following:

- Data Isolation and Explanation Fragmentation
  Client-side data distribution (non-IID) leads to local explanations that cannot be generalized. Sensor data from different factories in the IIoT may vary significantly in features, and traditional feature importance analysis might overestimate the impact of local noise [169].
- Privacy–Explainability Trade-off
  Enhancing explainability requires exposing details of model decisions (e.g., feature contributions) but may leak sensitive data information. VFL is particularly sensitive in the medical field. Reference [170] points out that explaining the association of patient features across institutions may expose privacy, necessitating the design of fine-grained access controls.
- Dynamic Model Heterogeneity
  The differences in client model architectures (e.g., resource-constrained devices using lightweight networks) make it difficult to unify explanation methods. When the CTFL framework [132] tracks rule activation patterns in heterogeneous models, the evaluation bias in contributions may occur due to differences in classification rules.

To address the above challenges, researchers target in-depth research on federated explainable technology:

- Privacy-Preserving Explanation Enhancement
  - Encryption and Feature Selection: The IP2FL model [130] combines additive homomorphic encryption (AHE) to protect gradient privacy, while utilizing Shapley values to quantify feature contributions, achieving high-trust anomaly detection in Industrial Cyber-Physical Systems (ICPSs). This framework optimizes system performance through dual feature selection while ensuring interpretive transparency.
  - Adaptive Gradient Protection (AGP): Reference [168] designs a selective noise injection mechanism that only perturbs channel parameters with minimal impact on explainability. It preserves the importance of key features while defending against gradient leakage attacks. Experiments show that this method can balance privacy and explainability under both IID and non-IID data.
- Causal Learning and Blockchain Auditing
  - Causal Sparsification: Reference [133] adopts a heterogeneous perception causal learning method, sparsifying weights that contribute less to model decisions, reducing communication costs and enhancing traceability. In medical image segmentation, only connections strongly related to pathological features are retained, assisting doctors in understanding the model's decision-making path.
  - Decentralized Data Quality Assessment: By integrating blockchain technology, the aggregation weights are dynamically adjusted to prioritize the integration of a high-quality data node explanation, enhancing the credibility of the global model [133].
- Multimodal and Rule-Driven Explanation
  - Multimodal Explanation Fusion: In [134], MRI, clinical, and psychological data are integrated into the prediction of Alzheimer's disease, using Shapley values to

explain the interaction of multimodal features. The global model AUC reaches 99.97%, and the contribution of key biomarkers (e.g., hippocampal atrophy) can be traced, assisting clinical decision-making.

- Efficient Contribution Estimation: Reference [132] proposed a contribution evaluation framework based on rule activation, which tracks the client's contribution to classification rules through a logistic neural network. It demonstrates significant accuracy and computational efficiency on four public classification datasets.

At the same time, the evaluation of federated explainability needs to combine technical characteristics and domain requirements:

- Clinical Verification
  In the medical field, reference [134] verifies the rationality of the model explanation through doctor blind testing to enhance the clinical adoption rate of diagnostic suggestions. The blockchain audit mechanism [133] enhances model credibility through data quality scoring.
- Industry Trustworthiness
  Reference [169] proposed a trustworthy federation framework for IIoT scenarios, verifying through a case study the impact of explainability on security decision-making (e.g., real-time response to anomaly detection results).
- Contribution Fairness
  The CTFL framework [132] evaluates the fairness of contribution allocation based on theoretical properties, such as symmetry and zero-element, and verifies the robustness through confrontation experiments.

Moreover, there are still the following controversies and open challenges for federated explainability:

- Privacy–Explainability Paradox
  Reference [170] points out that feature correlation explanation in vertical federations may leak cross-institutional user identities, necessitating the design of dynamic desensitization and access control strategies.
- Heterogeneous Rule Conflict
  CTFL [132] faces the problem of insufficient rule generalization under extreme non-IID scenarios and needs to combine meta-learning to optimize rule adaptability.
- Real-Time Constraints
  In industrial scenarios, encryption computations (e.g., IP2FL [130]) may increase the delay in generating explanations. There is a need to explore lightweight explanation frameworks to support real-time decision-making at the edge [135].

Table 4 compares the core technical directions and innovative points of explainability and privacy protection in FL. Research on the explainability of FL is evolving from a single model explanation to a multi-dimensional trustworthy framework, covering privacy protection, heterogeneous adaptation, and crossmodal alignment. However, data isolation and the complexity of dynamic environments remain core challenges. In the future, through lightweight design, causal inference, and collaborative optimization, it is necessary to build a transparent, efficient, and privacy-compliant federated explanation framework to achieve trustworthy decision support in key areas such as medical diagnosis and industrial control.

While robustness, fairness, and explainability are often discussed independently, they are deeply interrelated in practice. For instance, robust aggregation can mitigate malicious noise but may reduce fairness if lower-resource nodes are filtered out. Similarly, explainability mechanisms must navigate the trade-off between privacy protection and transparency. Understanding these interactions is crucial for designing holistic trust frameworks in federated systems.

Table 4. Comparison of key technologies for explainability and privacy protection in FL.

Research Direction	References	Main Findings	Research Significance
Explanation Enhancement under Privacy Protection	[130,168]	Ref. [130]: combining AHE with Shapley values to quantify feature contributions, achieving privacy protection and explainability in industrial control systems; Ref. [168]: AGP selectively perturbs low-impact channel parameters, balancing privacy with explainability.	While protecting data privacy, it provides trustworthy model explanations, meeting the compliance and decision-making transparency requirements in industrial and medical scenarios.
Causal Learning and Blockchain Integration	[133]	Heterogeneous perception causal learning sparsifies non-causal weights, reducing communication overhead and enhancing decision traceability; the blockchain dynamically evaluates data quality and optimizes aggregation weights.	This enhances the interpretability and credibility of models in scenarios such as medical image analysis, supporting the transparency of clinical decision-making.
Multimodal and Rule-Driven Explanation	[134,170]	Ref. [134]: multimodal data (MRI and clinical indicators) combined with Shapley explanation, achieving a global AUC of 99.97%; Ref. [170]: designing a fine-grained privacy–interpretability trade-off framework in VFL.	This addresses the issue of the fragmented explanation of crossmodal data, promoting trustworthy AI applications in multi-institutional collaboration in medical diagnosis.
Efficient Contribution Assessment Mechanism	[132]	Rule-based Activation Contribution Assessment (CTFL): single training inference completes contribution allocation; logical neural networks and binarization techniques ensure efficiency and privacy.	They motivate high-quality data providers to participate in FL, address the bias issue in heterogeneous model contributions assessment, and enhance collaboration fairness.
Trustworthy Verification Framework	[135,169]	Ref. [169]: an IIoT trustworthy federation framework with case validation of the impact of explainability on security decision-making; Ref. [135]: real-time edge anomaly detection (FedeX) combined with XAI explanation, which occupies only 14% of memory.	Enhances the credibility and real-time response capability of industrial control systems, supporting transparent deployment in resource-constrained scenarios.

5. Lightweight FL Framework for Resource-Constrained Edge–End Devices

5.1. Analysis of the Core Contradiction in Resource-Constrained FL

In resource-constrained FL scenarios, three key challenges arise. First, there is a dynamic trade-off between privacy protection, computational efficiency, and model accuracy. Second, communication constraints lead to multi-objective optimization dilemmas. Third, enhancing privacy protection often results in increased system entropy, reflecting growing complexity and resource demands (as shown in Table 5). Existing works have partially alleviated these contradictions through lightweight models, dynamic resource allocation, and hybrid encryption technologies, but further exploration of cross-layer collaborative optimization mechanisms is still needed.

5.1.1. Privacy–Efficiency–Accuracy Dynamic Game

In resource-constrained FL, the dynamic game between privacy protection, computational efficiency, and model accuracy constitutes a core contradiction. Traditional FL

frameworks assume that devices have abundant computing resources, but in reality, edge devices (e.g., industrial sensors and wearable devices) often face limitations in memory, computational power, and energy consumption, exacerbating the trade-offs between these objectives. The FedSens framework [38] alleviates the class imbalance problem in AHD through localized training and low-energy design, but sacrifices some global model accuracy to adapt to resource constraints. Similarly, the LDES framework [171] adopts sparsification and binarization of neural networks to reduce energy consumption, but after introducing DP, the convergence of the model is significantly affected, revealing the intrinsic conflict between privacy enhancement and accuracy loss.

Existing research attempts to alleviate this contradiction through lightweight encryption and dynamic resource allocation. The MEEC multi-key encryption framework [172] utilizes the lightweight EC-ElGamal algorithm to reduce communication overhead while ensuring privacy strength, but its adaptability in a heterogeneous device environment still needs verification. Although these methods have made progress in specific scenarios, the fundamental contradiction has not been completely resolved as follows: privacy protection mechanisms often introduce additional computational load, while lightweight designs (e.g., model pruning [173–175], quantization, and compressive [176,177]) may weaken the model's expressive power. Further exploration of adaptive privacy–efficiency–accuracy collaborative optimization mechanisms based on device capabilities is needed, such as dynamically adjusting the joint strategy of local training rounds and encryption strength.

Table 5. Key technology comparison of lightweight FL in resource-constrained environments.

Research Direction	References	Main Findings	Supporting Evidence	Research Significance
Combining Compressed Learning (CL) and FL	[176,178]	Integrating CL and FL, reducing computational and communication overheads, while preserving privacy.	Ref. [176]: computational overhead reduced by 66%, communication reduced by 99%, while accuracy still reaches 80%; Ref. [178]: using compressed sensing and DP, the feasibility of Raspberry Pi and Android devices is verified.	This resolves the contradiction between security and efficiency in resource-constrained IoT devices, promoting the practical application of edge computing and lightweight privacy protection.
Lightweight Models and Training Optimization	[171,179–181]	Reduction in local computing and communication burden through Sparse/Binary Neural Networks, model pruning, quantization, and other techniques.	Ref. [171]: the LDES algorithm reduces energy consumption by 56.21%; Ref. [180]: FedQNN compressed the model by more than 30 times, saving 90% of computational energy consumption; Ref. [181]: the GWEP method accelerates by 10.23 times.	It enhances the feasibility of edge devices participating in FL, reduces resource consumption, and expands the deployment scenarios of FL in low-performance terminals (e.g., IoT).
Blockchain-Enhanced Security in FL	[182–185]	Design of lightweight blockchain architectures (e.g., LiteChain and BEFL), combining digital signatures and consensus mechanisms to resist attacks.	Ref. [182]: proposed anti-counterfeiting signature algorithm; Ref. [183]: the LPBFL scheme reduces computational load through Paillier encryption and batch verification; Ref. [184]: LiteChain optimizes latency and storage.	It enhances the security of FL (resistance to poisoning and forgery attacks), meets industrial-grade privacy requirements, and supports dynamic user join/leave.

Table 5. *Cont.*

Research Direction	References	Main Findings	Supporting Evidence	Research Significance
Dynamic Resource Allocation and Heterogeneous Device Adaptation	[175,186–188]	Based on device capabilities, dynamically adjusting the model pruning rate, participation frequency, or resource allocation to optimize latency and energy consumption.	Ref. [186]: the Client Eligibility-based Lightweight Protocol (CELP) reduces communication overhead by 81%; Ref. [187]: the DDSRA algorithm balances training delay and accuracy; Ref. [175]: FedMP is accelerated by 4.1 times.	To address the disparities in the resources of heterogeneous devices, enhance the robustness of FL in dynamic network environments, and achieve efficient collaborative training.
Optimization for non-IID Data	[177,189,190]	Mitigates the issue of skewed data distribution through methods such as model splitting, bidirectional distillation (Bi-distillation), and prototype constraints.	Ref. [177]: FedAnil+ improves model accuracy by 13–26%; Ref. [189]: Double RL optimizes client selection and aggregation frequency; Ref. [190]: FedCPG achieves an average accuracy of 95%.	It addresses the issue of data heterogeneity in real-world scenarios, enhancing the usability of FL in industrial inspections, high-speed mobile networks, and other complex environments.
Communication Efficiency Improvement Strategies	[171,174,191,192]	Combining sparsification, quantification, and optimal model selection strategies (e.g., FedLamp) to compress communication data volume.	Ref. [191]: the PROBE algorithm supports the training of large-scale devices under bandwidth constraints; Ref. [192]: FedLamp reduces traffic by 63% and time by 52%.	Significantly reduces communication costs of FL, adapts to bandwidth-limited edge networks, and supports large-scale device collaboration.
Privacy Protection Enhancement Mechanisms	[172,178,182,193]	Design lightweight cryptographic schemes (e.g., dual-server architecture and EC-ElGamal encryption) or DP to protect local data.	Ref. [193]: resists collusion attacks, with only a marginal increase in communication overhead; Ref. [172]: MEEC supports multi-key collaborative computation, reducing communication failure rates.	While ensuring high accuracy, it also achieves strict privacy protection, making it suitable for sensitive scenarios such as healthcare and the IoT.
Optimization for Industrial and IoT Applications	[173,174,190,194]	Tailored lightweight FL solutions for scenarios such as industrial equipment fault detection (FedCPG), coal mine video surveillance (Rep-ShuffleNet), and network intrusion detection (Lightweight-Fed-NIDS).	Ref. [173]: model size reduced by 90%, training speed increased by 3 times; Ref. [194]: after optimization, YOLOv8 achieved an APsmall of 86.7%; Ref. [190]: memory usage reduced by 82%.	Promoting the implementation of FL in fields such as industrial automation and cybersecurity, addressing multiple challenges of real-time requirements, resource constraints, and high-precision demands.

5.1.2. Multi-Objective Optimization Dilemma Under Communication Constraints

The complexity of FL is further exacerbated by the communication bandwidth limitations and multi-objective optimization needs in resource-constrained environments. Typical problems include bandwidth pressure from high-dimensional gradient transmission, convergence speed differences due to device heterogeneity, and real-time requirements in latency-sensitive scenarios. The PROBE framework [191] resists channel attacks while reducing communication volume by combining over-the-air computing with gradient

sparsification and Gaussian perturbation, but its performance stability under non-IID data is insufficient. Meanwhile, the CELP protocol [186] adopts sample pruning and parameter reconfiguration techniques, reducing communication overhead by 81.01%, but sacrifices some model accuracy to adapt to resource-constrained devices.

The existing optimization paradigms mainly focus on a single objective (e.g., communication volume or energy consumption), neglecting the coupling relationship between multiple objectives. The FedLamp framework [192] balances communication cost and convergence speed by adaptively adjusting the local update frequency and model compression rate, but its dynamic decision-making mechanism depends on preset device capability parameters, making it difficult to cope with real-time changing network conditions. Therefore, there is a need to construct an end-to-end multi-objective joint optimization framework, integrating RL or meta-learning to achieve dynamic strategy generation, while considering the collaborative impact of device heterogeneity, data distribution differences, and latency constraints.

5.1.3. Increased System Entropy Triggered by Privacy Protection Enhancement

The introduction of privacy protection technology often leads to an "entropy increase effect" in system complexity and resource consumption. The blockchain-enabled FL (e.g., BEFL framework [185]) enhances security through the verifiable random function (VRF) consensus mechanism, but the on-chain storage and verification process significantly increases computational and communication overhead. The LPBFL scheme [183] uses Paillier encryption and batch verification to reduce the blockchain load, but its scalability is still limited in dynamic device join/leave scenarios.

While integrating the blockchain with FL enhances system trustworthiness, traceability, and robustness against poisoning attacks, it also inevitably introduces considerable system overhead. These include increased communication and storage consumption due to distributed ledger replication, computational load from cryptographic protocols such as homomorphic encryption or committee consensus, and possible trade-offs in convergence speed or model accuracy. Thus, although blockchain-enabled FL systems significantly enhance privacy and decentralization, these advantages come at the cost of increased system entropy—a term encapsulating the rising complexity, latency, and resource demands within the overall architecture.

This type of entropy increase effect is particularly prominent on lightweight devices. After reference [182] revealed the security vulnerabilities of existing signature schemes, the improved schemes increased security but further increased the computational burden on edge nodes. There is a need for further exploration of lightweight privacy protection architectures, based on distributed clustering (e.g., LiteChain [184]) or hybrid encryption (e.g., dual server protocol [193,195]), to reduce system complexity while ensuring security. In addition, cross-layer optimization techniques (e.g., IPFS storage and model compression collaboration) are expected to alleviate the storage pressure brought by the blockchain, providing new solutions for resource-constrained FL.

5.2. Optimization Paradigm for FL with Resource Constraints

5.2.1. Dynamic Resource-Aware FL Architecture

Addressing device heterogeneity and resource fluctuations, a dynamic resource-aware architecture becomes the core of optimization. The DDSRA framework [187] uses DNN partitioning technology to deploy shallow models on terminal devices, offloading deep models to edge gateways, and combining Lyapunov optimization to dynamically schedule device participation rates, achieving a Pareto-optimal balance between energy consumption and accuracy. The MEC-AI HetFL architecture [188] further introduces multi-edge cluster collabo-

ration and AI-driven node selection, allocating resources dynamically through quality scoring (Q-score), achieving a 5-fold performance improvement in heterogeneous environments.

Significant progress has also been made in the field of lightweight models. Reference [196] generates personalized lightweight models based on neural architecture search (NAS) and enhances resource adaptability by integrating Federated Mutual Learning. The GWEP framework [181] combines quantization and pruning to compress models, reducing communication volume by 90%. However, existing methods often rely on assumptions of static device capabilities, and there is an urgent need to develop real-time resource monitoring and elastic model adjustment mechanisms, such as dynamic load prediction technology based on DT.

5.2.2. Spatio-Temporal Decoupling Communication Optimization Mechanism

To address bandwidth limitations and latency constraints, spatio-temporal decoupling technology optimizes communication efficiency through gradient compression and asynchronous protocols. The edge–terminal collaboration framework [179] utilizes model migration to reduce latency. FedQNN [180] combines ultra-low bit quantization with sparsification to compress upstream and downstream data by 90%. The latency-aware asynchronous protocol (AAFL [148]) utilizes DRL to dynamically adjust aggregation frequency. This reduces the influence of long-tail devices and cuts training time by up to 70% under resource constraints.

However, the robustness of existing methods under non-IID data is insufficient. The three-tier federated reinforcement learning framework [189] optimizes client selection and aggregation frequency through a dual RL strategy, but its computational overhead limits deployment on lightweight devices. Further exploration of lightweight asynchronous protocols based on edge intelligence is needed, such as combining local gradient caching with priority scheduling to achieve the joint optimization of communication–computation–storage.

5.2.3. Privacy–Efficiency Collaborative Enhancement Technology

The collaborative optimization of privacy and efficiency is a core challenge for resource-constrained FL. The multi-objective NAS framework directly searches for Pareto-optimal model architectures on edge devices, balancing computational load with privacy intensity [197]; reference [178] combines compressed sensing with DP to achieve low-cost privacy protection on devices such as Raspberry Pi. Progress has also been made in vertical domain cases: the FedCPG framework [190] uses prototype constraints to guide personalized lightweight FL, achieving 95% accuracy in industrial fault detection. Reference [194] employs Rep-ShuffleNet to optimize YOLOv8, combined with asynchronous federation to reduce the delay in coal mine video detection.

Although hybrid schemes (e.g., lightweight encryption combined with model compression) have shown potential, their cross-layer optimization mechanisms are still immature. There is a need to further establish standardized evaluation metrics and benchmark testing platforms to quantify the trade-offs between privacy, efficiency, and accuracy. It is also necessary to explore new privacy protection paradigms (e.g., bidirectional distillation in FL [189]) to enhance model generalization without significantly increasing system complexity.

5.3. Evaluation Metrics and Benchmarking Considerations

To support the comparative analysis and reproducibility of FL frameworks in cloud–edge–end environments, it is crucial to summarize and standardize key evaluation metrics. These metrics offer measurable criteria for assessing existing architectures, as well as guiding future innovations. The following summarizes the most frequently used indicators in the literature:

- **Model Accuracy and Convergence:** Accuracy, precision, and recall are the most widely used performance indicators, with convergence speed and the number of rounds until convergence also frequently reported. For instance, the NSRA improved accuracy by 11.48% and 19.38% on MNIST and CIFAR-10 tasks, respectively [164].
- **Latency and Delay:** In real time and latency-sensitive applications, training and inference delays are measured. EAFL+ and MultiFed frameworks reduced latency through hierarchical and asynchronous mechanisms [63,68].
- **Communication Overhead:** Assessed by total transmitted data, the number of communication rounds, or bandwidth occupancy. The CELP reported 81.01% communication reduction via aggregation pruning and sparsification [186].
- **Energy Efficiency:** Measured as energy per round or per inference task, especially relevant to IoT devices. The LDES saved 56.21% energy consumption, while Eco-FL achieved up to 97% energy reduction compared to baseline methods [65,171].
- **Privacy and Security Metrics:** Privacy-preserving designs are evaluated through the differential privacy budget ϵ, leakage risk, or adversarial attack success rates. Works like the BEFL and PFLF frameworks quantify privacy–utility trade-offs [149,185].

A unified metric framework enables more transparent benchmarking and supports the construction of reproducible FL solutions. Future work should consider designing standardized benchmarking platforms for cross-layer collaborative systems, integrating real-time, multimodal, and trust-aware components.

6. Advanced Topics and Future Research Directions

6.1. Real-Time and Low-Latency FL

6.1.1. Online FL

Real-time or near-real-time FL has become an urgent need in the IoT, vehicle networks, and mobile scenarios. When data sources continuously surge in the form of streams, traditional static batch-style FL is unable to meet the requirements for continuous iteration and rapid response. Researchers have explored incremental training mechanisms to support continuous learning. These include fine-tuning models at the edge and using mini-batches for fast updates, all while maintaining low communication overhead. At the same time, the hybrid strategy of synchronous and asynchronous also receives attention: on the one hand, asynchronous training can enhance the flexibility of collaboration between devices, reducing the time fast devices wait for slow ones; on the other hand, if the delay in asynchronous aggregation is too large, significant divergences in model weights may occur during a global merge. Therefore, how to rationally utilize methods like "buffer-snapshot" to ensure model stability becomes a core research issue in online FL.

6.1.2. Latency Optimization for Edge/End–Side Inference

For scenarios such as AR/VR and autonomous driving that are extremely sensitive to latency, the main approach to reducing round-trip delay is to partially or completely offload the model inference to the edge/local side. However, this simultaneously poses challenges to computational resources and model complexity. In recent years, methods like model compression, operator fusion, and automatic neural architecture search (NAS) have provided directions for achieving efficient inference. Moreover, based on the cloud–edge–local hierarchical inference model, preliminary feature extraction is performed by local devices, while deep network inference is executed by edge servers. When the network condition is good, this can reduce the computational burden on the local side, and during congestion, it can flexibly switch to the local side to complete as much inference as possible. This multi-layer collaborative model has broad prospects in applications like AR/VR and

autonomous driving and also puts forward higher requirements for network scheduling and hardware acceleration.

6.2. Multimodal FL

6.2.1. Multi-Source Heterogeneous Data Fusion

Multimodal data fusion is an important means to enhance the robustness and explainability of AI decision-making. In scenarios such as intelligent healthcare and smart security, it is often necessary to process images, voice, text, and even biosensor data simultaneously. Due to the significant differences in the feature space and data distribution of each modality, the federated framework needs to perform feature extraction or auto-encoding at the device/edge–end, and use aggregation algorithms to align and fuse the latent representations in the cloud or at the edge. Such multimodal FL not only needs to focus on the accuracy of feature fusion but must also mitigate training biases arising from noisy or missing modalities. At the same time, crossmodal privacy protection has become a challenge. Most existing methods like DP and HE are designed for single modality, and future extensions are needed for higher-dimensional multimodal scenarios.

6.2.2. Synchronization and Alignment Issue

In multimodal FL, it is common for data from various modalities to arrive at different times and have inconsistent upload frequencies, leading to unavoidable asynchronous updates. If a key modality is delayed in uploading or encounters network congestion, ensuring the stability and consistency of the overall model at the aggregation moment is a focus of the current research. In terms of alignment, Early Fusion combines multiple modalities at the feature level in one step, while Late Fusion aggregates at the model decision level. Both approaches have their advantages. Late Fusion can better maintain independent updates of each modality in an asynchronous environment, thereby reducing noise interference. Moreover, it is necessary to strengthen robustness testing, simulating malicious attacks or abnormal data through methods such as artificial occlusion or noise injection, to evaluate the overall reliability of multimodal fusion.

6.3. Dynamic Resource Allocation and Adaptive Learning

6.3.1. Network and Node Dynamics

In real deployment environments, edge nodes often face issues such as insufficient power, mobility, and network fluctuations, which may go offline or rejoin at any time, causing instability in the federated training process. Bandwidth jitter and network congestion further exacerbate the difficulty of global model aggregation. On the one hand, researchers ensure the basic model iteration effect by reducing the aggregation frequency and waiting for nodes to upload in batches. On the other hand, they adopt a hierarchical multi-level aggregation strategy in the architecture to minimize bandwidth occupancy and tolerate some nodes going offline. At the same time, elastic fault tolerance mechanisms are proposed, such as using the latest snapshots or historical gradients when nodes fail or go online/offline, ensuring that the global model can still maintain a certain convergence speed and accuracy in the face of sudden changes.

6.3.2. Adaptive FL Framework

In response to the dynamic nature of the environment and the variability of tasks, researchers have begun to explore the integration of meta-learning or RL into the FL scheduling process. Specifically, by recording network statuses (e.g., bandwidth, latency, etc.), node statuses (e.g., uptime rate, battery level, computational capacity, etc.), and the convergence metrics of the current model during training, the RL agent can adaptively

select the optimal communication interval, compression ratio, node participation rate, and other hyperparameters. Such an adaptive framework can handle non-stationary data streams and highly dynamic network environments, enhancing the overall robustness and convergence efficiency of the model. In the future, adaptive FL will play a more crucial role in time-sensitive tasks like sudden disaster response and intelligent traffic scheduling.

7. Conclusions

With the rapid advancement of distributed intelligence, the cloud–edge–end collaboration architecture has become a foundational paradigm for enabling scalable, privacy-aware, and responsive AI applications. FL, as a decentralized training framework, offers unique advantages in preserving data locality and enhancing trust in collaborative environments. This review provides a comprehensive synthesis of current FL architectures tailored for cloud–edge–end collaboration, analyzing key technical challenges—including resource heterogeneity and non-IID data distributions—as well as emerging strategies for privacy preservation and lightweight deployment.

To distinguish our contributions, we introduce a three-dimensional trustworthiness framework for FL, encompassing data, processes, and outcome trust. This framework provides a conceptual lens to evaluate and strengthen federated workflows across system layers. We further explore the trilemma of privacy, efficiency, and accuracy and highlight adaptive optimization mechanisms designed to reconcile this trade-off under dynamic and constrained environments. Our analysis integrates discussions on real-time processing, multimodal data fusion, and trustworthy AI, all of which are pivotal for edge-intelligent systems in domains such as smart transportation and healthcare.

Looking ahead, future research should advance toward unified frameworks that combine secure model aggregation, causal explainability, and self-adaptive orchestration of FL across layers. Additionally, solving the interoperability challenges among heterogeneous devices and enabling real-time trustworthy learning from high-dimensional, multimodal, and incomplete data streams will be vital. These directions will help shape the next generation of federated intelligence, characterized by lightweight, trustworthy, and resilient learning systems deployed at scale.

Author Contributions: Conceptualization, S.Z. (Shanhao Zhan) and L.H.; investigation, S.Z. (Shanhao Zhan); writing—original draft preparation, S.Z. (Shanhao Zhan); writing—review and editing, Z.G., G.L. and S.Z. (Shaolong Zheng); supervision, H.-C.C. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Natural Science Foundation of China under Grant 62371406 and 62171392, in part by the Natural Science Foundation of Xiamen, China (Grant number 3502Z202473053), in part by the Science Technology Project of Fujian under Grant 2024H6030, in part by the Xiamen Science and Technology Subsidy Project (No. 2024CXY0318), and in part by the Key Laboratory of Digital Fujian on IoT Communication, Architecture, and Security Technology under Grant 2010499.

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:

FL	federated learning
PFL	personalized federated learning
BFL	Blockchain Federated Learning
VFL	Vertical Federated Learning
HFL	Horizontal Federated Learning
FTL	Federated Transfer Learning
BGFL	Blockchain-enhanced Grouped Federated Learning
KT	knowledge transfer
RL	reinforcement learning
DRL	deep reinforcement learning
RFL-HA	resource-efficient federated learning with hierarchical aggregation
AMVFL	asynchronous multi-party vertical federated learning
IID	independent and identically distributed
Non-IID	Non-Independent and Identically Distributed
IIoT	industrial Internet of Things
GCAE	generative convolutional autoencoder
HE	homomorphic encryption
AHE	additive homomorphic encryption
AGP	Adaptive Gradient Protection
ICPSs	Industrial Cyber-Physical Systems
AHD	abnormal health detection
DP	differential privacy
LDP	local differential privacy
UCB	Upper Confidence Bound
GAIN	Generative Adversarial Imputation Nets
GANs	Generative Adversarial Networks
VNE	virtual network embedding
DSA	dynamic security assessment
VEC	Vehicle Edge Computing
DAG	directed acyclic graph
HVAC	heating, ventilation, and air conditioning
FLR	Federated Logistic Regression
PSNR	peak signal-to-noise ratio
PCS	partial cosine similarity
IDSs	intrusion detection systems
DT	digital twin
DRAs	Data Reconstruction Attacks
MMFFC	Multimodal Multi-Feature Construction
AoU	Age of Update
CL	Compressed Learning
VRF	verifiable random function
CELP	Client Eligibility-based Lightweight Protocol

References

1. Letaief, K.B.; Chen, W.; Shi, Y.; Zhang, J.; Zhang, Y.J.A. The roadmap to 6G: AI empowered wireless networks. *IEEE Commun. Mag.* **2019**, *57*, 84–90. [CrossRef]
2. Noor-A-Rahim, M.; Liu, Z.; Lee, H.; Khyam, M.O.; He, J.; Pesch, D.; Moessner, K.; Saad, W.; Poor, H.V. 6G for vehicle-to-everything (V2X) communications: Enabling technologies, challenges, and opportunities. *Proc. IEEE* **2022**, *110*, 712–734. [CrossRef]
3. McMahan, B.; Moore, E.; Ramage, D.; Hampson, S.; Arcas, B.A.y. Communication-Efficient Learning of Deep Networks from Decentralized Data. In Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, PMLR, Fort Lauderdale, FL, USA , 20–22 April 2017; Volume 54, pp. 1273–1282.

4. Liu, S.; Liu, L.; Tang, J.; Yu, B.; Wang, Y.; Shi, W. Edge computing for autonomous driving: Opportunities and challenges. *Proc. IEEE* **2019**, *107*, 1697–1716. [CrossRef]
5. Baktir, A.C.; Ozgovde, A.; Ersoy, C. How Can Edge Computing Benefit From Software-Defined Networking: A Survey, Use Cases, and Future Directions. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2359–2391. [CrossRef]
6. Yuan, J.; Xiao, H.; Shen, Z.; Zhang, T.; Jin, J. ELECT: Energy-efficient intelligent edge–cloud collaboration for remote IoT services. *Future Gener. Comput. Syst.* **2023**, *147*, 179–194. [CrossRef]
7. Zolanvari, M.; Teixeira, M.A.; Gupta, L.; Khan, K.M.; Jain, R. Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things. *IEEE Internet Things J.* **2019**, *6*, 6822–6834. [CrossRef]
8. Moustafa, N.; Keshky, M.; Debiez, E.; Janicke, H. Federated TON-IoT Windows Datasets for Evaluating AI-Based Security Applications. In Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 29 December–1 January 2021; pp. 848–855. [CrossRef]
9. Al-Ansi, A.; Al-Ansi, A.M.; Muthanna, A.; Elgendy, I.A.; Koucheryavy, A. Survey on Intelligence Edge Computing in 6G: Characteristics, Challenges, Potential Use Cases, and Market Drivers. *Future Internet* **2021**, *13*, 118. [CrossRef]
10. Wang, Y.; Yang, S.; Ren, X.; Zhao, P.; Zhao, C.; Yang, X. IndustEdge: A Time-Sensitive Networking Enabled Edge-Cloud Collaborative Intelligent Platform for Smart Industry. *IEEE Trans. Ind. Inform.* **2022**, *18*, 2386–2398. [CrossRef]
11. Zhou, X.; Liang, W.; She, J.; Yan, Z.; Wang, K.I.K. Two-Layer Federated Learning with Heterogeneous Model Aggregation for 6G Supported Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2021**, *70*, 5308–5317. [CrossRef]
12. Liu, Z.; Du, H.; Hou, X.; Huang, L.; Hosseinalipour, S.; Niyato, D.; Letaief, K.B. Two-Timescale Model Caching and Resource Allocation for Edge-Enabled AI-Generated Content Services. *arXiv* **2024**, arXiv:2411.01458.
13. Duc, T.L.; Leiva, R.G.; Casari, P.; Östberg, P.O. Machine Learning Methods for Reliable Resource Provisioning in Edge-Cloud Computing: A Survey. *ACM Comput. Surv.* **2019**, *52*, 94. [CrossRef]
14. Hard, A.; Partridge, K.; Mathews, R.; Augenstein, S. Jointly learning from decentralized (federated) and centralized data to mitigate distribution shift. In Proceedings of the Neurips Workshop on Distribution Shifts, on the NeurIPS Virtual Site, Virtual, 13 December 2021.
15. Saad, W.; Bennis, M.; Chen, M. A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems. *IEEE Netw.* **2020**, *34*, 134–142. [CrossRef]
16. Chang, Z.; Liu, S.; Xiong, X.; Cai, Z.; Tu, G. A Survey of Recent Advances in Edge-Computing-Powered Artificial Intelligence of Things. *IEEE Internet Things J.* **2021**, *8*, 13849–13875. [CrossRef]
17. Yao, J.; Zhang, S.; Yao, Y.; Wang, F.; Ma, J.; Zhang, J.; Chu, Y.; Ji, L.; Jia, K.; Shen, T.; et al. Edge-Cloud Polarization and Collaboration: A Comprehensive Survey for AI. *IEEE Trans. Knowl. Data Eng.* **2023**, *35*, 6866–6886. [CrossRef]
18. Ren, J.; Zhang, D.; He, S.; Zhang, Y.; Li, T. A Survey on End-Edge-Cloud Orchestrated Network Computing Paradigms: Transparent Computing, Mobile Edge Computing, Fog Computing, and Cloudlet. *ACM Comput. Surv.* **2019**, *52*, 125. [CrossRef]
19. Xu, R.; Baracaldo, N.; Zhou, Y.; Anwar, A.; Kadhe, S.; Ludwig, H. DeTrust-FL: Privacy-Preserving Federated Learning in Decentralized Trust Setting. In Proceedings of the 2022 IEEE 15th International Conference on Cloud Computing (CLOUD), Barcelona, Spain, 10–16 July 2022; pp. 417–426. [CrossRef]
20. Jiang, Q.; Xu, X.; He, Q.; Zhang, X.; Dai, F.; Qi, L.; Dou, W. Game Theory-Based Task Offloading and Resource Allocation for Vehicular Networks in Edge-Cloud Computing. In Proceedings of the 2021 IEEE International Conference on Web Services (ICWS), Chicago, IL, USA, 5–10 September 2021; pp. 341–346. [CrossRef]
21. Sengupta, J.; Ruj, S.; Das Bit, S. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. *J. Netw. Comput. Appl.* **2020**, *149*, 102481. [CrossRef]
22. Tran, N.H.; Bao, W.; Zomaya, A.; Nguyen, M.N.H.; Hong, C.S. Federated Learning over Wireless Networks: Optimization Model Design and Analysis. In Proceedings of the IEEE INFOCOM 2019—IEEE Conference on Computer Communications, Paris, France, 29 April–2 May 2019; pp. 1387–1395. [CrossRef]
23. Fu, Y.; Li, C.; Yu, F.R.; Luan, T.H.; Zhao, P. An Incentive Mechanism of Incorporating Supervision Game for Federated Learning in Autonomous Driving. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 14800–14812. [CrossRef]
24. Zhou, Z.; Chen, X.; Li, E.; Zeng, L.; Luo, K.; Zhang, J. Edge Intelligence: Paving the Last Mile of Artificial Intelligence with Edge Computing. *Proc. IEEE* **2019**, *107*, 1738–1762. [CrossRef]
25. Ananthanarayanan, G.; Bahl, P.; Bodík, P.; Chintalapudi, K.; Philipose, M.; Ravindranath, L.; Sinha, S. Real-Time Video Analytics: The Killer App for Edge Computing. *Computer* **2017**, *50*, 58–67. [CrossRef]
26. 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]
27. Wu, Z.; Sun, S.; Wang, Y.; Liu, M.; Gao, B.; Pan, Q.; He, T.; Jiang, X. Agglomerative Federated Learning: Empowering Larger Model Training via End-Edge-Cloud Collaboration. In Proceedings of the IEEE INFOCOM 2024—IEEE Conference on Computer Communications, Vancouver, BC, Canada, 20–23 May 2024; pp. 131–140. [CrossRef]

28. Le, V.A.; Haga, J.; Tanimura, Y.; Nguyen, T.T. SFETEC: Split-FEderated Learning Scheme Optimized for Thing-Edge-Cloud Environment. In Proceedings of the 2024 IEEE 20th International Conference on e-Science (e-Science), Osaka, Japan, 16–20 September 2024; pp. 1–2. [CrossRef]
29. Li, C.; Yang, H.; Sun, Z.; Yao, Q.; Zhang, J.; Yu, A.; Vasilakos, A.V.; Liu, S.; Li, Y. High-Precision Cluster Federated Learning for Smart Home: An Edge-Cloud Collaboration Approach. *IEEE Access* **2023**, *11*, 102157–102168. [CrossRef]
30. Mhaisen, N.; Abdellatif, A.A.; Mohamed, A.; Erbad, A.; Guizani, M. Optimal User-Edge Assignment in Hierarchical Federated Learning Based on Statistical Properties and Network Topology Constraints. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 55–66. [CrossRef]
31. Ren, X.; Wang, Y.; Zhang, J.; Han, Z. Research on Edge-Cloud Collaborative Data Sharing Method Based on Federated Learning in Internet of Vehicles. In Proceedings of the 2023 IEEE 29th International Conference on Parallel and Distributed Systems (ICPADS), Ocean Flower Island, China, 17–21 December 2023; pp. 1075–1080. [CrossRef]
32. Yu, S.; Chen, X.; Zhou, Z.; Gong, X.; Wu, D. When Deep Reinforcement Learning Meets Federated Learning: Intelligent Multitimescale Resource Management for Multiaccess Edge Computing in 5G Ultradense Network. *IEEE Internet Things J.* **2021**, *8*, 2238–2251. [CrossRef]
33. Wang, Z.; Xu, H.; Liu, J.; Huang, H.; Qiao, C.; Zhao, Y. Resource-Efficient Federated Learning with Hierarchical Aggregation in Edge Computing. In Proceedings of the IEEE INFOCOM 2021—IEEE Conference on Computer Communications, Vancouver, BC, Canada, 10–13 May 2021; pp. 1–10. [CrossRef]
34. Wu, W.; He, L.; Lin, W.; Mao, R. Accelerating Federated Learning Over Reliability-Agnostic Clients in Mobile Edge Computing Systems. *IEEE Trans. Parallel Distrib. Syst.* **2021**, *32*, 1539–1551. [CrossRef]
35. Li, Z.; He, Y.; Yu, H.; Kang, J.; Li, X.; Xu, Z.; Niyato, D. Data Heterogeneity-Robust Federated Learning via Group Client Selection in Industrial IoT. *IEEE Internet Things J.* **2022**, *9*, 17844–17857. [CrossRef]
36. Lim, W.Y.B.; Ng, J.S.; Xiong, Z.; Jin, J.; Zhang, Y.; Niyato, D.; Leung, C.; Miao, C. Decentralized Edge Intelligence: A Dynamic Resource Allocation Framework for Hierarchical Federated Learning. *IEEE Trans. Parallel Distrib. Syst.* **2022**, *33*, 536–550. [CrossRef]
37. Wu, Q.; Chen, X.; Zhou, Z.; Zhang, J. FedHome: Cloud-Edge Based Personalized Federated Learning for In-Home Health Monitoring. *IEEE Trans. Mob. Comput.* **2022**, *21*, 2818–2832. [CrossRef]
38. Zhang, D.Y.; Kou, Z.; Wang, D. FedSens: A Federated Learning Approach for Smart Health Sensing with Class Imbalance in Resource Constrained Edge Computing. In Proceedings of the IEEE INFOCOM 2021—IEEE Conference on Computer Communications, Virtually, 10–13 May 2021; pp. 1–10. [CrossRef]
39. Huang, X.; Li, P.; Yu, R.; Wu, Y.; Xie, K.; Xie, S. FedParking: A Federated Learning Based Parking Space Estimation With Parked Vehicle Assisted Edge Computing. *IEEE Trans. Veh. Technol.* **2021**, *70*, 9355–9368. [CrossRef]
40. Ma, Q.; Zhang, Z.; Zhu, Z.; Zhao, Y. Cloud-Edge-End Collaboration Personalized Semi-supervised Federated Learning for Visual Localization. In Proceedings of the 2023 IEEE 29th International Conference on Parallel and Distributed Systems (ICPADS), Ocean Flower Island, China, 17–21 December 2023; pp. 2848–2849. [CrossRef]
41. Nguyen, D.C.; Hosseinalipour, S.; Love, D.J.; Pathirana, P.N.; Brinton, C.G. Latency Optimization for Blockchain-Empowered Federated Learning in Multi-Server Edge Computing. *IEEE J. Sel. Areas Commun.* **2022**, *40*, 3373–3390. [CrossRef]
42. Li, M.; Sun, P.; Zhou, H.; Zhao, L.; Liu, X.; Leung, V.C.M. Poster: Towards Accurate and Fast Federated Learning in End-Edge-Cloud Orchestrated Networks. In Proceedings of the 2023 IEEE 43rd International Conference on Distributed Computing Systems (ICDCS), Hong Kong, China, 18–21 July 2023; pp. 1–2. [CrossRef]
43. Prathiba, S.B.; Raja, G.; Anbalagan, S.; Dev, K.; Gurumoorthy, S.; Sankaran, A.P. Federated Learning Empowered Computation Offloading and Resource Management in 6G-V2X. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 3234–3243. [CrossRef]
44. Wu, Q.; Zhao, Y.; Fan, Q.; Fan, P.; Wang, J.; Zhang, C. Mobility-Aware Cooperative Caching in Vehicular Edge Computing Based on Asynchronous Federated and Deep Reinforcement Learning. *IEEE J. Sel. Top. Signal Process.* **2023**, *17*, 66–81. [CrossRef]
45. Kong, X.; Gao, H.; Shen, G.; Duan, G.; Das, S.K. FedVCP: A Federated-Learning-Based Cooperative Positioning Scheme for Social Internet of Vehicles. *IEEE Trans. Comput. Soc. Syst.* **2022**, *9*, 197–206. [CrossRef]
46. Zhang, X.; Tham, C.K.; Wang, W. Hierarchical Federated Learning with Edge Optimization in Constrained Networks. In Proceedings of the 2024 IEEE 99th Vehicular Technology Conference (VTC2024-Spring), Singapore, 24–27 June 2024; pp. 1–5. [CrossRef]
47. Benhelal, M.S.; Jouaber, B.; Afifi, H.; Moungla, H. SiamFLTP: Siamese Networks Empowered Federated Learning for Trajectory Prediction. In Proceedings of the 2024 International Wireless Communications and Mobile Computing (IWCMC), Ayia Napa, Cyprus, 27–31 May 2024; pp. 1106–1111. [CrossRef]
48. Li, X.; Cheng, L.; Sun, C.; Lam, K.Y.; Wang, X.; Li, F. Federated-Learning-Empowered Collaborative Data Sharing for Vehicular Edge Networks. *IEEE Netw.* **2021**, *35*, 116–124. [CrossRef]
49. Yuan, X.; Chen, J.; Yang, J.; Zhang, N.; Yang, T.; Han, T.; Taherkordi, A. FedSTN: Graph Representation Driven Federated Learning for Edge Computing Enabled Urban Traffic Flow Prediction. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 8738–8748. [CrossRef]

50. Liu, D.; Cui, E.; Shen, Y.; Ding, P.; Zhang, Z. Federated Learning Model Training Mechanism with Edge Cloud Collaboration for Services in Smart Cities. In Proceedings of the 2023 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), Beijing, China, 14–16 June 2023; pp. 1–5. [CrossRef]
51. Du, Z.; Zhang, G.; Zhang, Y.; Wei, W.; Chu, Z. Online Fine-tuning Method for Power Grid Artificial Intelligence Model Based on Cloud-Edge Collaboration. In Proceedings of the 2023 3rd International Conference on Robotics, Automation and Intelligent Control (ICRAIC), Zhangjiajie, China, 24–26 November 2023; pp. 72–76. [CrossRef]
52. Nguyen, D.C.; Ding, M.; Pathirana, P.N.; Seneviratne, A.; Zomaya, A.Y. Federated Learning for COVID-19 Detection with Generative Adversarial Networks in Edge Cloud Computing. *IEEE Internet Things J.* **2022**, *9*, 10257–10271. [CrossRef]
53. Qayyum, A.; Ahmad, K.; Ahsan, M.A.; Al-Fuqaha, A.; Qadir, J. Collaborative Federated Learning for Healthcare: Multi-Modal COVID-19 Diagnosis at the Edge. *IEEE Open J. Comput. Soc.* **2022**, *3*, 172–184. [CrossRef]
54. Hu, R.; Yang, R. Fedsemgan: A Semi-Supervised Federated Learning-Based Edge-Cloud Collaborative Framework for Medical Diagnosis Service. In Proceedings of the 2023 China Automation Congress (CAC), Chongqing, China, 17–19 November 2023; pp. 4051–4056. [CrossRef]
55. Kang, S.; Ros, S.; Song, I.; Tam, P.; Math, S.; Kim, S. Real-Time Prediction Algorithm for Intelligent Edge Networks with Federated Learning-Based Modeling. *Comput. Mater. Contin.* **2023**, *77*, 1967–1983. [CrossRef]
56. Daraghmi, Y.A.; Daraghmi, E.Y.; Daraghma, R.; Fouchal, H.; Ayaida, M. Edge–Fog–Cloud Computing Hierarchy for Improving Performance and Security of NB-IoT-Based Health Monitoring Systems. *Sensors* **2022**, *22*, 8646. [CrossRef]
57. Yao, Z.; Zhao, C. FedTMI: Knowledge aided federated transfer learning for industrial missing data imputation. *J. Process Control* **2022**, *117*, 206–215. [CrossRef]
58. Wei, Z.; Wang, J.; Zhao, Z.; Shi, K. Toward data efficient anomaly detection in heterogeneous edge–cloud environments using clustered federated learning. *Future Gener. Comput. Syst.* **2025**, *164*, 107559. [CrossRef]
59. Zhang, S.; Wang, X.; Zeng, R.; Zeng, C.; Li, Y.; Huang, M. A personalized federated cloud-edge collaboration framework via cross-client knowledge distillation. *Future Gener. Comput. Syst.* **2025**, *165*, 107594. [CrossRef]
60. Qin, T.; Cheng, G.; Wei, Y.; Yao, Z. Hier-SFL: Client-edge-cloud collaborative traffic classification framework based on hierarchical federated split learning. *Future Gener. Comput. Syst.* **2023**, *149*, 12–24. [CrossRef]
61. Su, L.; Li, Z. Incentive-driven long-term optimization for hierarchical federated learning. *Comput. Netw.* **2023**, *234*, 109944. [CrossRef]
62. Zhu, K.; Chen, W.; Jiao, L.; Wang, J.; Peng, Y.; Zhang, L. Online training data acquisition for federated learning in cloud–edge networks. *Comput. Netw.* **2023**, *223*, 109556. [CrossRef]
63. Arouj, A.; Abdelmoniem, A.M. Towards Energy-Aware Federated Learning via Collaborative Computing Approach. *Comput. Commun.* **2024**, *221*, 131–141. [CrossRef]
64. Li, D.; Lai, J.; Wang, R.; Li, X.; Vijayakumar, P.; Gupta, B.B.; Alhalabi, W. Ubiquitous intelligent federated learning privacy-preserving scheme under edge computing. *Future Gener. Comput. Syst.* **2023**, *144*, 205–218. [CrossRef]
65. Savoia, M.; Prezioso, E.; Mele, V.; Piccialli, F. Eco-FL: Enhancing Federated Learning sustainability in edge computing through energy-efficient client selection. *Comput. Commun.* **2024**, *225*, 156–170. [CrossRef]
66. Mazzocca, C.; Romandini, N.; Montanari, R.; Bellavista, P. Enabling Federated Learning at the Edge through the IOTA Tangle. *Future Gener. Comput. Syst.* **2024**, *152*, 17–29. [CrossRef]
67. Parra-Ullauri, J.M.; Madhukumar, H.; Nicolaescu, A.C.; Zhang, X.; Bravalheri, A.; Hussain, R.; Vasilakos, X.; Nejabati, R.; Simeonidou, D. kubeFlower: A privacy-preserving framework for Kubernetes-based federated learning in cloud–edge environments. *Future Gener. Comput. Syst.* **2024**, *157*, 558–572. [CrossRef]
68. Xu, J.; Lin, J.; Li, Y.; Xu, Z. MultiFed: A fast converging federated learning framework for services QoS prediction via cloud–edge collaboration mechanism. *Knowl.-Based Syst.* **2023**, *268*, 110463. [CrossRef]
69. Xu, X.; Liu, W.; Zhang, Y.; Zhang, X.; Dou, W.; Qi, L.; Bhuiyan, M.Z.A. PSDF: Privacy-aware IoV Service Deployment with Federated Learning in Cloud-Edge Computing. *ACM Trans. Intell. Syst. Technol.* **2022**, *13*, 70. [CrossRef]
70. Yang, J.; Zheng, J.; Zhang, Z.; Chen, Q.I.; Wong, D.S.; Li, Y. Security of federated learning for cloud-edge intelligence collaborative computing. *Int. J. Intell. Syst.* **2022**, *37*, 9290–9308. [CrossRef]
71. Zhao, L.; Ni, S.; Wu, D.; Zhou, L. Cloud-Edge-Client Collaborative Learning in Digital Twin Empowered Mobile Networks. *IEEE J. Sel. Areas Commun.* **2023**, *41*, 3491–3503. [CrossRef]
72. Shi, L.; Shu, J.; Zhang, W.; Liu, Y. HFL-DP: Hierarchical Federated Learning with Differential Privacy. In Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December 2021; pp. 1–7. [CrossRef]
73. Zhang, L.; Xu, J.; Sivaraman, A.; Deborah Lazarus, J.; Sharma, P.K.; Pandi, V. A Two-Stage Differential Privacy Scheme for Federated Learning Based on Edge Intelligence. *IEEE J. Biomed. Health Inform.* **2024**, *28*, 3349–3360. [CrossRef]
74. Yang, J.; Zheng, J.; Baker, T.; Tang, S.; Tan, Y.a.; Zhang, Q. Clean-label poisoning attacks on federated learning for IoT. *Expert Syst.* **2023**, *40*, e13161. [CrossRef]

75. Zhou, Y.; Wang, R.; Mo, X.; Li, Z.; Tang, T. Robust Hierarchical Federated Learning with Anomaly Detection in Cloud-Edge-End Cooperation Networks. *Electronics* **2023**, *12*, 112. [CrossRef]
76. Aouedi, O.; Piamrat, K.; Muller, G.; Singh, K. Intrusion detection for Softwarized Networks with Semi-supervised Federated Learning. In Proceedings of the ICC 2022—IEEE International Conference on Communications, Seoul, Republic of Korea, 16–20 May 2022; pp. 5244–5249. [CrossRef]
77. Huong, T.T.; Bac, T.P.; Long, D.M.; Thang, B.D.; Binh, N.T.; Luong, T.D.; Phuc, T.K. LocKedge: Low-Complexity Cyberattack Detection in IoT Edge Computing. *IEEE Access* **2021**, *9*, 29696–29710. [CrossRef]
78. Wang, Z.; Wang, S.; Zhao, Z.; Sun, M. Trustworthy Localization with EM-Based Federated Control Scheme for IIoTs. *IEEE Trans. Ind. Inform.* **2023**, *19*, 1069–1079. [CrossRef]
79. Xia, F.; Chen, Y.; Huang, J. Privacy-preserving task offloading in mobile edge computing: A deep reinforcement learning approach. *Softw. Pract. Exp.* **2024**, *54*, 1774–1792. [CrossRef]
80. Chen, X.; Xu, G.; Xu, X.; Jiang, H.; Tian, Z.; Ma, T. Multicenter Hierarchical Federated Learning with Fault-Tolerance Mechanisms for Resilient Edge Computing Networks. *IEEE Trans. Neural Netw. Learn. Syst.* **2025**, *36*, 47–61. [CrossRef]
81. Math, S.; Tam, P.; Kim, S. Reliable Federated Learning Systems Based on Intelligent Resource Sharing Scheme for Big Data Internet of Things. *IEEE Access* **2021**, *9*, 108091–108100. [CrossRef]
82. Truong, V.T.; Hoang, D.N.M.; Le, L.B. BFLMeta: Blockchain-Empowered Metaverse with Byzantine-Robust Federated Learning. In Proceedings of the GLOBECOM 2023—2023 IEEE Global Communications Conference, Kuala Lumpur, Malaysia, 4–8 December 2023; pp. 5537–5542. [CrossRef]
83. Peng, G.; Shi, X.; Zhang, J.; Gao, L.; Tan, Y.; Xiang, N.; Wang, W. BGFL: A blockchain-enabled group federated learning at wireless industrial edges. *J. Cloud Comput.* **2024**, *13*, 148. [CrossRef]
84. Wu, F.; Li, X.; Li, J.; Vijayakumar, P.; Gupta, B.B.; Arya, V. HSADR: A New Highly Secure Aggregation and Dropout-Resilient Federated Learning Scheme for Radio Access Networks with Edge Computing Systems. *IEEE Trans. Green Commun. Netw.* **2024**, *8*, 1141–1155. [CrossRef]
85. Wang, J.; Chang, X.; Mišić, J.; Mišić, V.B.; Chen, Z.; Fan, J. PA-iMFL: Communication-Efficient Privacy Amplification Method Against Data Reconstruction Attack in Improved Multilayer Federated Learning. *IEEE Internet Things J.* **2024**, *11*, 17960–17974. [CrossRef]
86. Ma, X.; He, X.; Wu, X.; Wen, C. Multi-level federated learning based on cloud-edge-client collaboration and outlier-tolerance for fault diagnosis. *Meas. Sci. Technol.* **2023**, *34*, 125148. [CrossRef]
87. Mahanipour, A.; Khamfroush, H. Multimodal Multiple Federated Feature Construction Method for IoT Environments. In Proceedings of the GLOBECOM 2023—2023 IEEE Global Communications Conference, Kuala Lumpur, Malaysia, 4–8 December 2023; pp. 1890–1895. [CrossRef]
88. Yang, Z.; Fu, S.; Bao, W.; Yuan, D.; Zomaya, A.Y. Hierarchical Federated Learning with Momentum Acceleration in Multi-Tier Networks. *IEEE Trans. Parallel Distrib. Syst.* **2023**, *34*, 2629–2641. [CrossRef]
89. Luo, L.; Zhang, C.; Yu, H.; Sun, G.; Luo, S.; Dustdar, S. Communication-Efficient Federated Learning with Adaptive Aggregation for Heterogeneous Client-Edge-Cloud Network. *IEEE Trans. Serv. Comput.* **2024**, *17*, 3241–3255. [CrossRef]
90. Ma, C.; Li, X.; Huang, B.; Li, G.; Li, F. Personalized client-edge-cloud hierarchical federated learning in mobile edge computing. *J. Cloud Comput.* **2024**, *13*, 161. [CrossRef]
91. Liu, J.; Liu, X.; Wei, X.; Gao, H.; Wang, Y. Group Formation and Sampling in Group-Based Hierarchical Federated Learning. *IEEE Trans. Cloud Comput.* **2024**, *12*, 1433–1448. [CrossRef]
92. Zheng, Z.; Hong, Y.; Xie, X.; Li, K.; Chen, Q. A multi-dimensional incentive mechanism based on age of update in hierarchical federated learning. *Softw. Pract. Exp.* **2025**, *55*, 383–406. [CrossRef]
93. Liu, L.; Zhang, J.; Song, S.; Letaief, K.B. Client-Edge-Cloud Hierarchical Federated Learning. In Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC), Virtual, 7–11 June 2020; pp. 1–6. [CrossRef]
94. Hu, X.; Zhu, X.; Yang, L.; Pedrycz, W.; Li, Z. A Design of Fuzzy Rule-Based Classifier for Multiclass Classification and Its Realization in Horizontal Federated Learning. *IEEE Trans. Fuzzy Syst.* **2024**, *32*, 5098–5108. [CrossRef]
95. Yang, Y.; He, D.; Wang, J.; Feng, Q.; Luo, M. EPDR: An Efficient and Privacy-Preserving Disease Research System with Horizontal Federated Learning in the Internet of Medical Things. *Hum.-Centric Comput. Inf. Sci.* **2024**, *14*, 7. [CrossRef]
96. Sumitra; Shenoy, M.V. HFedDI: A novel privacy preserving horizontal federated learning based scheme for IoT device identification. *J. Netw. Comput. Appl.* **2023**, *214*, 103616. [CrossRef]
97. Zhang, Z.; Li, Y.; Zhang, K. EHFL: Efficient Horizontal Federated Learning with Privacy Protection and Verifiable Aggregation. *IEEE Internet Things J.* **2024**, *11*, 36884–36894. [CrossRef]
98. Ren, C.; Wang, T.; Yu, H.; Xu, Y.; Dong, Z.Y. EFedDSA: An Efficient Differential Privacy-Based Horizontal Federated Learning Approach for Smart Grid Dynamic Security Assessment. *IEEE J. Emerg. Sel. Top. Circuits Syst.* **2023**, *13*, 817–828. [CrossRef]
99. Wang, R.; Qiu, H.; Gao, H.; Li, C.; Dong, Z.Y.; Liu, J. Adaptive Horizontal Federated Learning-Based Demand Response Baseline Load Estimation. *IEEE Trans. Smart Grid* **2024**, *15*, 1659–1669. [CrossRef]

100. Zhang, X.; Mavromatis, A.; Vafeas, A.; Nejabati, R.; Simeonidou, D. Federated Feature Selection for Horizontal Federated Learning in IoT Networks. *IEEE Internet Things J.* **2023**, *10*, 10095–10112. [CrossRef]
101. Zhang, P.; Chen, N.; Li, S.; Choo, K.K.R.; Jiang, C.; Wu, S. Multi-Domain Virtual Network Embedding Algorithm Based on Horizontal Federated Learning. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 3363–3375. [CrossRef]
102. Cheng, K.; Fan, T.; Jin, Y.; Liu, Y.; Chen, T.; Papadopoulos, D.; Yang, Q. SecureBoost: A Lossless Federated Learning Framework. *IEEE Intell. Syst.* **2021**, *36*, 87–98. [CrossRef]
103. Errounda, F.Z.; Liu, Y. Adaptive differential privacy in vertical federated learning for mobility forecasting. *Future Gener. Comput. Syst.* **2023**, *149*, 531–546. [CrossRef]
104. Wang, R.; Ersoy, O.; Zhu, H.; Jin, Y.; Liang, K. FEVERLESS: Fast and Secure Vertical Federated Learning Based on XGBoost for Decentralized Labels. *IEEE Trans. Big Data* **2024**, *10*, 1001–1015. [CrossRef]
105. Yang, Y.; Chen, X.; Pan, Y.; Shen, J.; Cao, Z.; Dong, X.; Li, X.; Sun, J.; Yang, G.; Deng, R. OpenVFL: A Vertical Federated Learning Framework with Stronger Privacy-Preserving. *IEEE Trans. Inf. Forensics Secur.* **2024**, *19*, 9670–9681. [CrossRef]
106. Xu, W.; Zhu, H.; Zheng, Y.; Wang, F.; Zhao, J.; Liu, Z.; Li, H. ELXGB: An Efficient and Privacy-Preserving XGBoost for Vertical Federated Learning. *IEEE Trans. Serv. Comput.* **2024**, *17*, 878–892. [CrossRef]
107. Wang, G.; Zhang, Q.; Li, X.; Wang, B.; Gu, B.; Ling, C.X. Secure and fast asynchronous Vertical Federated Learning via cascaded hybrid optimization. *Mach. Learn.* **2024**, *113*, 6413–6451. [CrossRef]
108. Xuan, Y.; Chen, X.; Zhao, Z.; Tang, B.; Dong, Y. Practical and General Backdoor Attacks Against Vertical Federated Learning. In Proceedings of the Machine Learning and Knowledge Discovery in Databases: Research Track, Turin, Italy, 18–22 September 2023; pp. 402–417.
109. Chen, P.; Du, X.; Lu, Z.; Chai, H. Universal adversarial backdoor attacks to fool vertical federated learning. *Comput. Secur.* **2024**, *137*, 103601. [CrossRef]
110. Zhu, D.; Chen, J.; Zhou, X.; Shang, W.; Hassan, A.E.; Grossklags, J. Vulnerabilities of Data Protection in Vertical Federated Learning Training and Countermeasures. *IEEE Trans. Inf. Forensics Secur.* **2024**, *19*, 3674–3689. [CrossRef]
111. Ding, L.; Bao, H.; Lv, Q.; Zhang, F.; Zhang, Z.; Han, J.; Ding, S. Threshold Filtering for Detecting Label Inference Attacks in Vertical Federated Learning. *Electronics* **2024**, *13*, 4376. [CrossRef]
112. Shi, H.; Xu, Y.; Jiang, Y.; Yu, H.; Cui, L. Efficient Asynchronous Multi-Participant Vertical Federated Learning. *IEEE Trans. Big Data* **2024**, *10*, 940–952. [CrossRef]
113. Cai, D.; Fan, T.; Kang, Y.; Fan, L.; Xu, M.; Wang, S.; Yang, Q. Accelerating Vertical Federated Learning. *IEEE Trans. Big Data* **2024**, *10*, 752–760. [CrossRef]
114. Wu, Z.; Li, Q.; He, B. Practical Vertical Federated Learning with Unsupervised Representation Learning. *IEEE Trans. Big Data* **2024**, *10*, 864–878. [CrossRef]
115. Yan, Y.; Wang, H.; Huang, Y.; He, N.; Zhu, L.; Xu, Y.; Li, Y.; Zheng, Y. Cross-Modal Vertical Federated Learning for MRI Reconstruction. *IEEE J. Biomed. Health Inform.* **2024**, *28*, 6384–6394. [CrossRef] [PubMed]
116. Li, P.; Guo, C.; Xing, Y.; Shi, Y.; Feng, L.; Zhou, F. Core network traffic prediction based on vertical federated learning and split learning. *Sci. Rep.* **2024**, *14*, 4663. [CrossRef]
117. Zhang, R.; Li, H.; Tian, L.; Hao, M.; Zhang, Y. Vertical Federated Learning Across Heterogeneous Regions for Industry 4.0. *IEEE Trans. Ind. Inform.* **2024**, *20*, 10145–10155. [CrossRef]
118. Liu, Y.; Kang, Y.; Xing, C.; Chen, T.; Yang, Q. A Secure Federated Transfer Learning Framework. *IEEE Intell. Syst.* **2020**, *35*, 70–82. [CrossRef]
119. Qi, T.; Wu, F.; Wu, C.; He, L.; Huang, Y.; Xie, X. Differentially private knowledge transfer for federated learning. *Nat. Commun.* **2023**, *14*, 3785. [CrossRef] [PubMed]
120. Jin, X.; Bu, J.; Yu, Z.; Zhang, H.; Wang, Y. FedCrack: Federated Transfer Learning with Unsupervised Representation for Crack Detection. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 11171–11184. [CrossRef]
121. Wang, Z.; Xiao, J.; Wang, L.; Yao, J. A novel federated learning approach with knowledge transfer for credit scoring. *Decis. Support Syst.* **2024**, *177*, 114084. [CrossRef]
122. Li, K.; Lu, J.; Zuo, H.; Zhang, G. Federated Fuzzy Transfer Learning with Domain and Category Shifts. *IEEE Trans. Fuzzy Syst.* **2024**, *32*, 6708–6719. [CrossRef]
123. Mao, W.; Yu, B.; Zhang, C.; Qin, A.; Xie, Y. FedKT: Federated learning with knowledge transfer for non-IID data. *Pattern Recognit.* **2025**, *159*, 111143. [CrossRef]
124. Dang, Q.; Zhang, G.; Wang, L.; Yang, S.; Zhan, T. Hybrid IoT Device Selection with Knowledge Transfer for Federated Learning. *IEEE Internet Things J.* **2024**, *11*, 12216–12227. [CrossRef]
125. Li, Z.; Li, Z.; Gu, F. Intelligent diagnosis method for machine faults based on federated transfer learning. *Appl. Soft Comput.* **2024**, *163*, 111922. [CrossRef]
126. Xu, D.; Liu, Y.; Wen, G.; Jin, Y.; Chai, T.; Yang, T. DeFedTL: A Decentralized Federated Transfer Learning Method for Fault Diagnosis. *IEEE Trans. Ind. Inform.* **2025**, *21*, 1704–1713. [CrossRef]

127. Singh, G.; Bedi, J. A federated and transfer learning based approach for households load forecasting. *Knowl.-Based Syst.* **2024**, *299*, 111967. [CrossRef]
128. Wang, Z.; Yu, P.; Zhang, H. Privacy-Preserving Regulation Capacity Evaluation for HVAC Systems in Heterogeneous Buildings Based on Federated Learning and Transfer Learning. *IEEE Trans. Smart Grid* **2023**, *14*, 3535–3549. [CrossRef]
129. Alharbi, A.A. Federated transfer learning for attack detection for Internet of Medical Things. *Int. J. Inf. Secur.* **2024**, *23*, 81–100. [CrossRef]
130. Namakshenas, D.; Yazdinejad, A.; Dehghantanha, A.; Parizi, R.M.; Srivastava, G. IP2FL: Interpretation-Based Privacy-Preserving Federated Learning for Industrial Cyber-Physical Systems. *IEEE Trans. Ind. Cyber-Phys. Syst.* **2024**, *2*, 321–330. [CrossRef]
131. Qin, Z.; Yang, L.; Wang, Q.; Han, Y.; Hu, Q. Reliable and Interpretable Personalized Federated Learning. In Proceedings of the 2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Vancouver, BC, Canada, 17–24 June 2023; pp. 20422–20431. [CrossRef]
132. Wang, Y.; Li, K.; Luo, Y.; Li, G.; Guo, Y.; Wang, Z. Fast, Robust and Interpretable Participant Contribution Estimation for Federated Learning. In Proceedings of the 2024 IEEE 40th International Conference on Data Engineering (ICDE), Utrecht, The Netherlands, 13–16 May 2024; pp. 2298–2311. [CrossRef]
133. Mu, J.; Kadoch, M.; Yuan, T.; Lv, W.; Liu, Q.; Li, B. Explainable Federated Medical Image Analysis Through Causal Learning and Blockchain. *IEEE J. Biomed. Health Inform.* **2024**, *28*, 3206–3218. [CrossRef]
134. Jahan, S.; Saif Adib, M.R.; Huda, S.M.; Rahman, M.S.; Kaiser, M.S.; Sanwar Hosen, A.S.M.; Ghimire, D.; Park, M.J. Federated Explainable AI-Based Alzheimer's Disease Prediction with Multimodal Data. *IEEE Access* **2025**, *13*, 43435–43454. [CrossRef]
135. Huong, T.T.; Bac, T.P.; Ha, K.N.; Hoang, N.V.; Hoang, N.X.; Hung, N.T.; Tran, K.P. Federated Learning-Based Explainable Anomaly Detection for Industrial Control Systems. *IEEE Access* **2022**, *10*, 53854–53872. [CrossRef]
136. Wu, W.; He, L.; Lin, W.; Mao, R.; Maple, C.; Jarvis, S. SAFA: A Semi-Asynchronous Protocol for Fast Federated Learning with Low Overhead. *IEEE Trans. Comput.* **2021**, *70*, 655–668. [CrossRef]
137. Blanchard, P.; El Mhamdi, E.M.; Guerraoui, R.; Stainer, J. Machine learning with adversaries: Byzantine tolerant gradient descent. In Proceedings of the 31st International Conference on Neural Information Processing Systems, NIPS'17, Red Hook, NY, USA, 4–9 December 2017; pp. 118–128.
138. Sun, Z.; Kairouz, P.; Suresh, A.T.; McMahan, H.B. Can You Really Backdoor Federated Learning? *arXiv* **2019**, arXiv:1911.07963. [CrossRef]
139. Liu, Y.; Garg, S.; Nie, J.; Zhang, Y.; Xiong, Z.; Kang, J.; Hossain, M.S. Deep Anomaly Detection for Time-Series Data in Industrial IoT: A Communication-Efficient On-Device Federated Learning Approach. *IEEE Internet Things J.* **2021**, *8*, 6348–6358. [CrossRef]
140. Qian, B.; Zhao, Y.; Tang, J.; Wang, Z.; Li, F.; Wang, J.; He, S.; Liu, J. Robust Federated Learning with Valid Gradient Direction for Cloud-Edge-End Collaboration in Smart Grids. In Proceedings of the 2024 International Conference on Energy and Electrical Engineering (EEE), Nanchang, China, 5–6 July 2024; pp. 1–5. [CrossRef]
141. Wang, L.; Xu, Y.; Xu, H.; Chen, M.; Huang, L. Accelerating Decentralized Federated Learning in Heterogeneous Edge Computing. *IEEE Trans. Mob. Comput.* **2023**, *22*, 5001–5016. [CrossRef]
142. Li, Y.; Zhou, Y.; Jolfaei, A.; Yu, D.; Xu, G.; Zheng, X. Privacy-Preserving Federated Learning Framework Based on Chained Secure Multiparty Computing. *IEEE Internet Things J.* **2021**, *8*, 6178–6186. [CrossRef]
143. Zhao, Y.; Zhao, J.; Jiang, L.; Tan, R.; Niyato, D.; Li, Z.; Lyu, L.; Liu, Y. Privacy-Preserving Blockchain-Based Federated Learning for IoT Devices. *IEEE Internet Things J.* **2021**, *8*, 1817–1829. [CrossRef]
144. Ji, Z.; Chen, L.; Zhao, N.; Chen, Y.; Wei, G.; Yu, F.R. Computation Offloading for Edge-Assisted Federated Learning. *IEEE Trans. Veh. Technol.* **2021**, *70*, 9330–9344. [CrossRef]
145. Jiang, Z.; Xu, Y.; Xu, H.; Wang, Z.; Qiao, C.; Zhao, Y. FedMP: Federated Learning through Adaptive Model Pruning in Heterogeneous Edge Computing. In Proceedings of the 2022 IEEE 38th International Conference on Data Engineering (ICDE), Virtual, 9–12 May 2022; pp. 767–779. [CrossRef]
146. Zhang, J.; Chen, B.; Cheng, X.; Binh, H.T.T.; Yu, S. PoisonGAN: Generative Poisoning Attacks Against Federated Learning in Edge Computing Systems. *IEEE Internet Things J.* **2021**, *8*, 3310–3322. [CrossRef]
147. Wang, T.; Liu, Y.; Zheng, X.; Dai, H.N.; Jia, W.; Xie, M. Edge-Based Communication Optimization for Distributed Federated Learning. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 2015–2024. [CrossRef]
148. Liu, J.; Xu, H.; Wang, L.; Xu, Y.; Qian, C.; Huang, J.; Huang, H. Adaptive Asynchronous Federated Learning in Resource-Constrained Edge Computing. *IEEE Trans. Mob. Comput.* **2023**, *22*, 674–690. [CrossRef]
149. Zhou, H.; Yang, G.; Dai, H.; Liu, G. PFLF: Privacy-Preserving Federated Learning Framework for Edge Computing. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 1905–1918. [CrossRef]
150. Wang, Y.; Su, Z.; Zhang, N.; Benslimane, A. Learning in the Air: Secure Federated Learning for UAV-Assisted Crowdsensing. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 1055–1069. [CrossRef]
151. Xiao, H.; Zhao, J.; Pei, Q.; Feng, J.; Liu, L.; Shi, W. Vehicle Selection and Resource Optimization for Federated Learning in Vehicular Edge Computing. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 11073–11087. [CrossRef]

152. Shinde, S.S.; Bozorgchenani, A.; Tarchi, D.; Ni, Q. On the Design of Federated Learning in Latency and Energy Constrained Computation Offloading Operations in Vehicular Edge Computing Systems. *IEEE Trans. Veh. Technol.* **2022**, *71*, 2041–2057. [CrossRef]
153. Zhang, F.; Zhai, D.; Bai, G.; Jiang, J.; Ye, Q.; Ji, X.; Liu, X. Towards fairness-aware and privacy-preserving enhanced collaborative learning for healthcare. *Nat. Commun.* **2025**, *16*, 2852. [CrossRef] [PubMed]
154. Su, Z.; Wang, Y.; Luan, T.H.; Zhang, N.; Li, F.; Chen, T.; Cao, H. Secure and Efficient Federated Learning for Smart Grid with Edge-Cloud Collaboration. *IEEE Trans. Ind. Inform.* **2022**, *18*, 1333–1344. [CrossRef]
155. Chen, D.; Hong, C.S.; Wang, L.; Zha, Y.; Zhang, Y.; Liu, X.; Han, Z. Matching-Theory-Based Low-Latency Scheme for Multitask Federated Learning in MEC Networks. *IEEE Internet Things J.* **2021**, *8*, 11415–11426. [CrossRef]
156. Feng, L.; Yang, Z.; Guo, S.; Qiu, X.; Li, W.; Yu, P. Two-Layered Blockchain Architecture for Federated Learning Over the Mobile Edge Network. *IEEE Netw.* **2022**, *36*, 45–51. [CrossRef]
157. Wang, X.; Zhao, Y.; Qiu, C.; Liu, Z.; Nie, J.; Leung, V.C.M. InFEDge: A Blockchain-Based Incentive Mechanism in Hierarchical Federated Learning for End-Edge-Cloud Communications. *IEEE J. Sel. Areas Commun.* **2022**, *40*, 3325–3342. [CrossRef]
158. Qu, Y.; Yu, S.; Gao, L.; Sood, K.; Xiang, Y. Blockchained Dual-Asynchronous Federated Learning Services for Digital Twin Empowered Edge-Cloud Continuum. *IEEE Trans. Serv. Comput.* **2024**, *17*, 836–849. [CrossRef]
159. Ahmed, K.M.; Imteaj, A.; Amini, M.H. Federated Deep Learning for Heterogeneous Edge Computing. In Proceedings of the 2021 20th IEEE International Conference on Machine Learning and Applications (ICMLA), Virtual, 13–16 December 2021; pp. 1146–1152. [CrossRef]
160. Liu, Y.; Jiang, L.; Qi, Q.; Xie, S. Energy-Efficient Space–Air–Ground Integrated Edge Computing for Internet of Remote Things: A Federated DRL Approach. *IEEE Internet Things J.* **2023**, *10*, 4845–4856. [CrossRef]
161. Mohri, M.; Sivek, G.; Suresh, A.T. Agnostic Federated Learning. In Proceedings of Machine Learning Research, Proceedings of the 36th International Conference on Machine Learning, Long Beach, CA, USA, 9–15 June 2019; Chaudhuri, K., Salakhutdinov, R., Eds.; PMLR: Cambridge, MA, USA, 2019; Volume 97, pp. 4615–4625.
162. Liu, T.; Di, B.; An, P.; Song, L. Privacy-Preserving Incentive Mechanism Design for Federated Cloud-Edge Learning. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 2588–2600. [CrossRef]
163. Xu, C.; Wu, Q. Research on Blockchain Privacy Computing Technology for End-edge-cloud Collaborative Architecture. In Proceedings of the 2023 4th Information Communication Technologies Conference (ICTC), Nanjing, China, 17–19 May 2023; pp. 316–320. [CrossRef]
164. Xin, S.; Zhuo, L.; Xin, C. Node Selection Strategy Design Based on Reputation Mechanism for Hierarchical Federated Learning. In Proceedings of the 2022 18th International Conference on Mobility, Sensing and Networking (MSN), Guangzhou, China, 14–16 December 2022; pp. 718–722. [CrossRef]
165. Zhao, Y.; Liu, Z.; Qiu, C.; Wang, X.; Yu, F.R.; Leung, V.C. An Incentive Mechanism for Big Data Trading in End-Edge-Cloud Hierarchical Federated Learning. In Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December 2021; pp. 1–6. [CrossRef]
166. Ribeiro, M.T.; Singh, S.; Guestrin, C. "Why Should I Trust You?": Explaining the Predictions of Any Classifier. In Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD '16, New York, NY, USA, 13–17 August 2016; pp. 1135–1144. [CrossRef]
167. Rozemberczki, B.; Watson, L.; Bayer, P.; Yang, H.T.; Kiss, O.; Nilsson, S.; Sarkar, R. The Shapley Value in Machine Learning. In Proceedings of the 31st International Joint Conference on Artificial Intelligence and the 25th European Conference on Artificial Intelligence, IJCAI-ECAI 2022, Vienna, Austria, 23–29 July 2022; pp. 5572–5579. [CrossRef]
168. Li, Z.; Chen, H.; Ni, Z.; Gao, Y.; Lou, W. Towards Adaptive Privacy Protection for Interpretable Federated Learning. *IEEE Trans. Mob. Comput.* **2024**, *23*, 14471–14483. [CrossRef]
169. Jagatheesaperumal, S.K.; Rahouti, M.; Alfatemi, A.; Ghani, N.; Quy, V.K.; Chehri, A. Enabling Trustworthy Federated Learning in Industrial IoT: Bridging the Gap Between Interpretability and Robustness. *IEEE Internet Things Mag.* **2024**, *7*, 38–44. [CrossRef]
170. Sakib, S.K.; Das, A.B. Explainable Vertical Federated Learning for Healthcare: Ensuring Privacy and Optimal Accuracy. In Proceedings of the 2024 IEEE International Conference on Big Data (BigData), Washington, DC, USA, 15–18 December 2024; pp. 5068–5077. [CrossRef]
171. Lei, L.; Yuan, Y.; Zhou, Y.; Yang, Y.; Luo, Y.; Pu, L.; Chatzinotas, S. Energy Optimization and Lightweight Design for Efficient Federated Learning in Wireless Edge Systems. *IEEE Trans. Veh. Technol.* **2024**, *73*, 13542–13557. [CrossRef]
172. Chen, Y.; Liu, L.; Ping, Y.; Atiquzzaman, M.; Mumtaz, S.; Zhang, Z.; Guizani, M.; Tian, Z. A Privacy-Preserving Federated Learning Framework with Lightweight and Fair in IoT. *IEEE Trans. Netw. Serv. Manag.* **2024**, *21*, 5843–5858. [CrossRef]
173. Bouayad, A.; Alami, H.; Janati Idrissi, M.; Berrada, I. Lightweight Federated Learning for Efficient Network Intrusion Detection. *IEEE Access* **2024**, *12*, 172027–172045. [CrossRef]
174. Du, J.; Qin, N.; Huang, D.; Jia, X.; Zhang, Y. Lightweight FL: A Low-Cost Federated Learning Framework for Mechanical Fault Diagnosis with Training Optimization and Model Pruning. *IEEE Trans. Instrum. Meas.* **2024**, *73*, 3504014. [CrossRef]

175. Jiang, Z.; Xu, Y.; Xu, H.; Wang, Z.; Liu, J.; Chen, Q.; Qiao, C. Computation and Communication Efficient Federated Learning with Adaptive Model Pruning. *IEEE Trans. Mob. Comput.* **2024**, *23*, 2003–2021. [CrossRef]
176. Gao, X.; Hou, L.; Chen, B.; Yao, X.; Suo, Z. Compressive-Learning-Based Federated Learning for Intelligent IoT with Cloud–Edge Collaboration. *IEEE Internet Things J.* **2025**, *12*, 2291–2294. [CrossRef]
177. Fotohi, R.; Shams Aliee, F.; Farahani, B. A Lightweight and Secure Deep Learning Model for Privacy-Preserving Federated Learning in Intelligent Enterprises. *IEEE Internet Things J.* **2024**, *11*, 31988–31998. [CrossRef]
178. Hidayat, M.A.; Nakamura, Y.; Arakawa, Y. Efficient and Secure: Privacy-Preserving Federated Learning for Resource-Constrained Devices. In Proceedings of the 2023 24th IEEE International Conference on Mobile Data Management (MDM), Singapore, 3–6 July 2023; pp. 184–187. [CrossRef]
179. Yuan, P.; Huang, R.; Zhang, J.; Zhang, E.; Zhao, X. Accuracy Rate Maximization in Edge Federated Learning with Delay and Energy Constraints. *IEEE Syst. J.* **2023**, *17*, 2053–2064. [CrossRef]
180. Ji, Y.; Chen, L. FedQNN: A Computation–Communication-Efficient Federated Learning Framework for IoT with Low-Bitwidth Neural Network Quantization. *IEEE Internet Things J.* **2023**, *10*, 2494–2507. [CrossRef]
181. Prakash, P.; Ding, J.; Chen, R.; Qin, X.; Shu, M.; Cui, Q.; Guo, Y.; Pan, M. IoT Device Friendly and Communication-Efficient Federated Learning via Joint Model Pruning and Quantization. *IEEE Internet Things J.* **2022**, *9*, 13638–13650. [CrossRef]
182. Sui, Z.; Sun, Y.; Zhu, J.; Chen, F. Comments on "Lightweight Privacy and Security Computing for Blockchained Federated Learning in IoT". *IEEE Internet Things J.* **2024**, *11*, 15043–15046. [CrossRef]
183. Fan, M.; Ji, K.; Zhang, Z.; Yu, H.; Sun, G. Lightweight Privacy and Security Computing for Blockchained Federated Learning in IoT. *IEEE Internet Things J.* **2023**, *10*, 16048–16060. [CrossRef]
184. Chen, H.; Zhou, R.; Chan, Y.H.; Jiang, Z.; Chen, X.; Ngai, E.C.H. LiteChain: A Lightweight Blockchain for Verifiable and Scalable Federated Learning in Massive Edge Networks. *IEEE Trans. Mob. Comput.* **2025**, *24*, 1928–1944. [CrossRef]
185. Jin, R.; Hu, J.; Min, G.; Mills, J. Lightweight Blockchain-Empowered Secure and Efficient Federated Edge Learning. *IEEE Trans. Comput.* **2023**, *72*, 3314–3325. [CrossRef]
186. Asad, M.; Otoum, S.; Shaukat, S. Clients Eligibility-Based Lightweight Protocol in Federated Learning: An IDS Use Case. *IEEE Trans. Netw. Serv. Manag.* **2024**, *21*, 3759–3774. [CrossRef]
187. Deng, X.; Li, J.; Ma, C.; Wei, K.; Shi, L.; Ding, M.; Chen, W. Low-Latency Federated Learning with DNN Partition in Distributed Industrial IoT Networks. *IEEE J. Sel. Areas Commun.* **2023**, *41*, 755–775. [CrossRef]
188. Mughal, F.R.; He, J.; Das, B.; Dharejo, F.A.; Zhu, N.; Khan, S.B.; Alzahrani, S. Adaptive federated learning for resource-constrained IoT devices through edge intelligence and multi-edge clustering. *Sci. Rep.* **2024**, *14*, 28746. [CrossRef]
189. Zhou, X.; Zheng, X.; Cui, X.; Shi, J.; Liang, W.; Yan, Z.; Yang, L.T.; Shimizu, S.; Wang, K.I.K. Digital Twin Enhanced Federated Reinforcement Learning with Lightweight Knowledge Distillation in Mobile Networks. *IEEE J. Sel. Areas Commun.* **2023**, *41*, 3191–3211. [CrossRef]
190. Li, H.; Wang, X.; Cao, P.; Li, Y.; Yi, B.; Huang, M. FedCPG: A class prototype guided personalized lightweight federated learning framework for cross-factory fault detection. *Comput. Ind.* **2025**, *164*, 104180. [CrossRef]
191. Tao, Y.; Chen, S.; Zhang, C.; Wang, D.; Yu, D.; Cheng, X.; Dressler, F. Private Over-the-Air Federated Learning at Band-Limited Edge. *IEEE Trans. Mob. Comput.* **2024**, *23*, 12444–12460. [CrossRef]
192. Xu, Y.; Liao, Y.; Xu, H.; Ma, Z.; Wang, L.; Liu, J. Adaptive Control of Local Updating and Model Compression for Efficient Federated Learning. *IEEE Trans. Mob. Comput.* **2023**, *22*, 5675–5689. [CrossRef]
193. Zhong, L.; Wang, L.; Zhang, L.; Domingo-Ferrer, J.; Xu, L.; Wu, C.; Zhang, R. Dual-Server-Based Lightweight Privacy-Preserving Federated Learning. *IEEE Trans. Netw. Serv. Manag.* **2024**, *21*, 4787–4800. [CrossRef]
194. Wu, J.; Zheng, R.; Jiang, J.; Tian, Z.; Chen, W.; Wang, Z.; Yu, F.R.; Leung, V.C.M. A Lightweight Small Object Detection Method Based on Multilayer Coordination Federated Intelligence for Coal Mine IoVT. *IEEE Internet Things J.* **2024**, *11*, 20072–20087. [CrossRef]
195. Zhang, Z.; Wu, L.; Ma, C.; Li, J.; Wang, J.; Wang, Q.; Yu, S. LSFL: A Lightweight and Secure Federated Learning Scheme for Edge Computing. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 365–379. [CrossRef]
196. Li, Y.; Yao, R.; Qin, D.; Wang, Y. Lightweight Federated Learning for On-Device Non-Intrusive Load Monitoring. *IEEE Trans. Smart Grid* **2025**, *16*, 1950–1961. [CrossRef]
197. Lyu, B.; Yuan, H.; Lu, L.; Zhang, Y. Resource-Constrained Neural Architecture Search on Edge Devices. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 134–142. [CrossRef]