Review

Synergizing Intelligence and Privacy: A Review of Integrating Internet of Things, Large Language Models, and Federated Learning in Advanced Networked Systems

Hongming Yang , Hao Liu , Xin Yuan , Kai Wu , Wei Ni * , J. Andrew Zhang , Ren Ping Liu

Posted Date: 24 April 2025

doi: 10.20944/preprints202504.2082.v1

Keywords: Internet of Things (IoT); LLMs; Federated Learning (FL); Privacy-Preserving Techniques (PETs); Edge Computing; Parameter-Efficient Fine-Tuning (PEFT); Split Federated Learning (SFL); Data Heterogeneity; Network Security; Distributed Systems

 doi:10.20944/preprints202504.2082.v1

Article

Synergizing Intelligence and Privacy: A Review of Integrating Internet of Things, Large Language Models, and Federated Learning in Advanced Networked Systems

Hongming Yang [1,†], Hao Liu [1,†], Xin Yuan [2,†], Kai Wu [1,3,†], Wei Ni [2,*], J. Andrew Zhang [1,3,†] and Ren Ping Liu [1,3,†]

[1] School of Electrical and Data Engineering (SEDE), University of Technology Sydney (UTS), Sydney, NSW 2007, Australia
[2] Data61, Commonwealth Scientific and Industrial Research Organization, Marsfield, NSW 2122, Australia
[3] Global Big Data Technologies Centre (GBDTC), University of Technology Sydney (UTS), Sydney, NSW 2007, Australia
* Correspondence: wei.ni@ieee.org
† These authors contributed equally to this work.

Abstract: Bringing together the Internet of Things (IoT), LLMs , and Federated Learning (FL) offers exciting possibilities, creating a synergy to build smarter, privacy-preserving distributed systems. This review explores the merging of these technologies, particularly within edge computing environments. We examine current architectures and practical methods enabling this fusion, such as efficient low-rank adaptation (LoRA) for fine-tuning large models and memory-efficient Split Federated Learning (SFL) for collaborative edge training. However, this integration faces significant hurdles: the resource limitations of IoT devices, unreliable network communication, data heterogeneity, diverse security threats, fairness considerations, and regulatory demands. While other surveys cover pairwise combinations, this review distinctively analyzes the three-way synergy, highlighting how IoT, LLMs, and FL working in concert unlock capabilities unattainable otherwise. Our analysis compares various strategies proposed to tackle these issues (e.g., federated vs. centralized, SFL vs. standard FL, DP vs. cryptographic privacy), outlining their practical trade-offs. We showcase real-world progress and potential applications in domains like Industrial IoT and Smart Cities, considering both opportunities and limitations. Finally, this review identifies critical open questions and promising future research paths, including ultra-lightweight models, robust algorithms for heterogeneity, machine unlearning, standardized benchmarks, novel FL paradigms, and next-generation security. Addressing these areas is essential for responsibly harnessing this powerful technological blend.

Keywords: Internet of Things (IoT); LLMs ; Federated Learning (FL); privacy-preserving techniques (PETs); edge computing; Parameter-Efficient Fine-Tuning (PEFT); Split Federated Learning (SFL); data heterogeneity; network security; distributed systems

1. Introduction

1.1. Background

IoT and Artificial Intelligence (AI) are reshaping the way we live. IoT is penetrating to every aspect of our modern society. It features the explosion of interconnected devices generating vast amounts of real-world data, driving significant and innovative insights to improve our life. Simultaneously, the emerging LLMs like the GPT series have shown a remarkable ability to understand and process complex information [1,2]. The power of LLMs arises from a vast amount of training data, while IoT systems are excellent means to provide such data. Combining the two fields is a natural move. This, however, incurs significant challenges. A core question is that how can we leverage the intelligence of resource-hungry LLMs to make sense of the massive, diverse, and often sensitive data streams produced by countless IoT devices, especially when the data is mostly heterogeneous, multi-modality,

 doi:10.20944/preprints202504.2082.v1

high-dimensional, sparse, and needs to be processed quickly and, in many cases, locally [3–5]. This is further elaborated on below.

1.2. Motivation

Sending huge volumes of IoT data to a central cloud for AI analysis often isn't practical [6]. It can be too slow for applications needing real-time responses (like industrial control or autonomous systems); consumes too much bandwidth; and raises significant privacy concerns [7]. Many critical IoT applications simply demand intelligence closer to the data source [3]. On the other hand, while LLMs possess the analytical power needed for complex IoT tasks, they face their own hurdles: they require massive datasets for training, and accessing the rich, real-world, but often private, data held on distributed IoT devices is difficult [8]. Moreover, deploying these powerful models effectively within the constraints of real-world distributed systems like IoT remains a significant challenge, considering limited hardware resources and power supply, data access, and privacy. This is precisely where FL enters the picture [9]. FL revolutionizes traditional approaches by enabling collaborative model training across decentralized data sources, eliminating the need for raw data centralization. This creates a compelling opportunity: using FL to train powerful LLMs on diverse, distributed IoT data while preserving user privacy and data locality [10,11]. This combination promises smarter, more responsive, and privacy-respecting systems, potentially leading to more efficient factories, safer autonomous vehicles, or more personalized healthcare, all leveraging local data securely. However, integrating these three sophisticated technologies (IoT, LLMs, FL) creates unique complexities and challenges related to efficiency, security, fairness, and scalability [12]. Given the significance of the integration and the increasing attention it has gained recently, this review aims to provide a timely overview of the state-of-the-art in synergizing IoT, LLMs, and FL, particularly for edge environments, hoping to highlight current capabilities, identify key challenges, and inspire future research directions that enable intelligent, privacy-preserving, and resource-efficient edge intelligence systems. Specifically, we will explore the architectures, methods, inherent challenges, and promising solutions, highlighting why this three-way integration is crucial for building the next generation of intelligent, distributed systems.

1.3. Scope and Contribution

The burgeoning interest in deploying advanced AI models like LLMs within distributed environments like IoT, often facilitated by techniques such as FL and edge computing, has spurred a number of valuable survey papers. While these reviews provide essential insights, they typically focus on specific sub-domains or pairwise interactions. Some representative survey works are reviewed below. Table 1 summarizes their primary focus and key differentiating aspects alongside our current work.

- Qu et al. [13] focuses on how Mobile Edge Intelligence (MEI) infrastructure can *support* the deployment (caching, delivery, training, inference) of LLMs, emphasizing resource efficiency in mobile networks. Their core contribution lies in detailing MEI mechanisms specifically tailored for LLMs, especially in caching and delivery, within a 6G context.
- Adam et al. [14] provides a comprehensive overview of *FL applied to the broad domain of IoT*, covering FL fundamentals, diverse IoT applications (healthcare, smart cities, autonomous driving), architectures (CFL, HFL, DFL), a detailed FL-IoT taxonomy, and challenges like heterogeneity and resource constraints. LLMs are treated as an emerging FL trend within the IoT ecosystem.
- Friha et al. [15] examines the integration of *LLMs as a core component of Edge Intelligence (EI)*, detailing architectures, optimization strategies (e.g., compression, caching), applications (driving, software engineering, healthcare, etc.), and offering an extensive analysis of the security and trustworthiness aspects specific to deploying LLMs at the edge.
- Cheng et al. [10] specifically targets the intersection of *FL and LLMs*, providing an exhaustive review of motivations, methodologies (pre-training, fine-tuning, Parameter-Efficient Fine-Tuning (PEFT), backpropagation-free), privacy (DP, HE, SMPC), and robustness (Byzantine, poisoning,

 doi:10.20944/preprints202504.2082.v1

prompt attacks) within the "Federated LLM" paradigm, largely independent of the specific application domain (like IoT) or deployment infrastructure (like MEI).

Table 1. Comparison with Related Surveys.

Survey	Primary Focus	Key Strengths	Distinction from Our Work
Qu et al. [13]	MEI supporting LLMs	Deep dive into edge resource optimization (compute, comms, storage); Mobile network context (6G); Detailed edge caching/delivery for LLMs.	Focuses on infrastructure *for* LLMs; Less depth on FL specifics, security/trust, or the unique *synergy* of IoT+LLM+FL. Less emphasis on IoT data characteristics.
Adam et al. [14]	FL for IoT Applications	Comprehensive FL principles in IoT context; Detailed IoT application case studies; Broad FL taxonomy for IoT.	IoT application-driven; LLMs are only one emerging aspect; Less depth on LLM specifics or the challenges arising from the three-way synergy.
Friha et al. [15]	LLMs integrated into EI	Deep analysis of security and trustworthiness for LLM-based EI; Covers architectures, optimization, autonomy, applications broadly.	Focuses on LLM *as* EI component; Less depth on FL methods specifically for training LLMs on distributed *IoT* data.
Cheng et al. [10]	Federated LLMs (FL + LLM)	Exhaustive review of FL methods for LLMs (PEFT, init, etc.); Deep dive into privacy/robustness specific to Federated LLMs.	Focuses narrowly on FL+LLM interaction; Less emphasis on the specific *IoT context* (data types, device constraints) or the *edge infrastructure* aspects.
This Survey	**Synergy of IoT + LLM + FL for Privacy-Preserving Edge Intelligence**	**Unique focus on the three-way interaction;** Explicit analysis of synergistic effects (Section 5); Addresses challenges arising specifically from the integration; Compares trade-offs in the specific IoT+LLM+FL@Edge context.	Provides a holistic view of the integration, bridging gaps between surveys focused on pairwise interactions or single components. Emphasizes the unique capabilities, privacy considerations, and challenges born from the *specific combination* of IoT data richness, LLM intelligence, and FL's distributed privacy paradigm within advanced edge networks.

While prior reviews cover areas like edge resources for LLMs [13], FL for IoT [14], edge LLM security [15], or federated LLM methods [10], they mainly look at pairs of these technologies. This survey distinctively examines the combined power and challenges of integrating all three, including IoT, LLMs, and FL, particularly for privacy-focused intelligence at the network edge. This synergy is depicted in Figure 1. It illustrates a conceptual framework in which synergistic AI solutions emerge from the integration of IoT, LLMs, FL, and PETs. Each component contributes uniquely, where IoT provides pervasive data sources, LLMs offer powerful reasoning and language capabilities, FL supports decentralized learning, and PETs ensure data confidentiality, together forming a foundation for scalable, intelligent, and privacy-aware edge AI systems.

 doi:10.20944/preprints202504.2082.v1

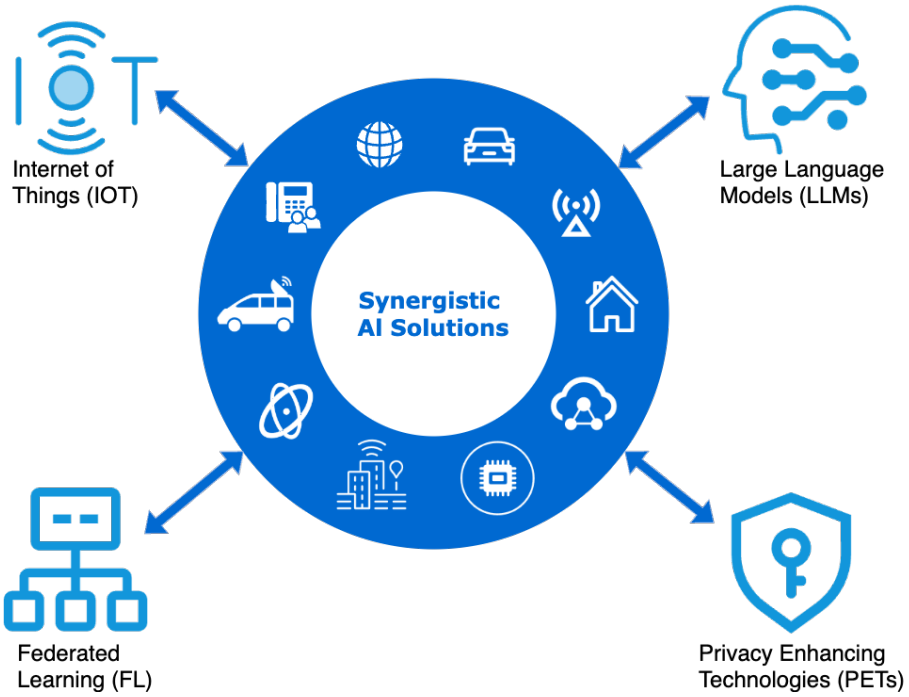

Figure 1. Conceptual overview of the technological convergence enabling synergistic AI solutions through the integration of IoT, LLMs, FL, and PETs.

More specifically, this review provides a comprehensive analysis of the state-of-the-art regarding architectures, methodologies, challenges, and potential solutions for integrating IoT, LLMs, and FL, with a specific emphasis on achieving privacy-preserving intelligence in edge computing environments. We explore architectural paradigms conducive to edge deployment based on [3], investigate key enabling techniques including PEFT methods like LoRA [16] and distributed training strategies such as SFL [17,18], and systematically analyze the inherent multifaceted challenges spanning resource constraints, communication efficiency, data/system heterogeneity, privacy/security threats, fairness, and scalability [3]. Mitigation strategies are discussed alongside critical comparisons highlighting advantages and Disadvantages. We survey recent applications to illustrate practical relevance [19]. While existing surveys may cover subsets of this intersection, such as FL for IoT [20,21] or FL for LLMs [22], this review offers a unique contribution by focusing specifically on the three-way synergy (IoT + LLM + FL) and its implications for privacy-preserving edge intelligence [10]. We aim to provide a structured taxonomy of relevant techniques, critically compare their suitability for resource-constrained and distributed IoT settings, identify research gaps specifically arising from this unique technological confluence, and propose targeted future research directions essential for advancing the field of trustworthy, decentralized AI [23].

As summarized in Figure 2, the subsequent sections are structured as follows: Section 2 introduces foundational concepts related to IoT systems, LLMs, FL principles, and PETs. Section 3 discusses architectural considerations for deploying LLMs within IoT ecosystems. Section 4 examines FL methodologies specifically adapted for LLM training and fine-tuning in this context, including frameworks and data considerations. Section 5 analyzes the unique synergistic effects arising from the integration of IoT, LLMs, and FL, highlighting emergent capabilities. Section 6 provides an expanded analysis of key challenges encountered in the integration, discusses mitigation strategies, and evaluates inherent trade-offs. Section 7 identifies critical research gaps and elaborates on future research directions stemming from the synergistic integration. Section 8 concludes the review, summarizing the key insights and forward-looking perspectives on privacy-preserving, intelligent distributed systems enabled by IoT, LLMs, and FL.

 doi:10.20944/preprints202504.2082.v1

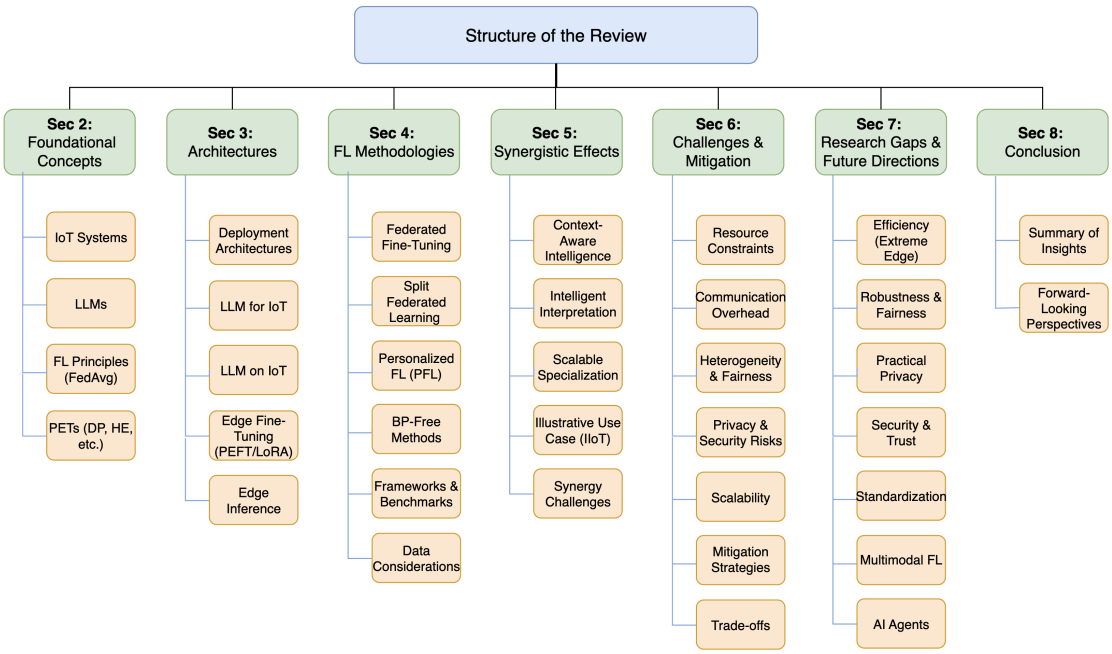

Figure 2. Overview of the review structure, detailing the main sections and key topics covered.

2. Foundational Concepts

2.1. IoT in Advanced Networks

IoT encompasses vast networks of interconnected devices, characterized by massive scale, significant heterogeneity (in terms of hardware capabilities, power sources, connectivity, data types), real-time data generation, and a strong trend towards edge computing for localized processing [6,24,25]. The inherent resource limitations (such as CPU, memory, battery) of many end devices represent a primary bottleneck for executing complex AI models directly at the extreme edge [26].

2.2. Large Language Models (LLMs)

LLMs are deep learning models, primarily Transformer-based [27], possessing billions of parameters and demonstrating powerful emergent capabilities derived from extensive pre-training [1,28]. They typically undergo fine-tuning for task adaptation [29]. Their significant size imposes high computational costs for training and inference, making deployment on standard IoT hardware challenging [4]. Ethical considerations regarding potential biases and responsible use are also critical [5,30].

2.3. Federated Learning (FL)

FL enables collaborative training on decentralized data [9]. The most widely known FL algorithm is Federated Averaging (FedAvg) [9,31,32]. In each communication round t, local clients receive the current global model weights $\mathbf{w}_t$ from the central server. K selected clients then train the model locally using its data D_k for E epochs, and update local weights $\mathbf{w}_{t+1}^k, k \in K$. The server aggregates these local weights to produce the updated global model $\mathbf{w}_{t+1}$ as

$$\mathbf{w}_{t+1} \leftarrow \sum_{k=1}^{K} \frac{n_k}{n} \mathbf{w}_{t+1}^k, \tag{1}$$

where $n_k = |D_k|$ is the number of data points on client k, and $n = \sum_{k=1}^{K} n_k$ is the total number of data points across the selected clients [33]. This weighted average aims to give more importance to updates from clients with more data. The adoption of FL, particularly in sensitive or distributed environments like IoT, is driven by several key advantages over traditional centralized approaches [7]:

- **Enhanced Privacy:** Data remains localized on user devices, reducing risks associated with central data aggregation.

 doi:10.20944/preprints202504.2082.v1

- **Communication Efficiency:** Transmitting model updates instead of raw data significantly reduces network load.
- **Utilizing Distributed Resources:** Leverages the computational power available at the edge devices [34].

While FedAvg provides a foundational approach, practical FL implementations involve several key characteristics, architectural choices, and challenges:

- **CFL vs. DFL:** Centralized FL (CFL) uses a server for coordination and aggregation, offering simplicity but creating a potential bottleneck and single point of failure [35]. Decentralized FL (DFL) employs peer-to-peer communication, potentially increasing robustness and scalability for certain network topologies (like mesh networks common in IoT scenarios) but adding complexity in coordination and convergence analysis [36].
- **Non-IID Data:** A central challenge in FL stems from heterogeneous data distributions across clients, commonly referred to as Non-Independent and Identically Distributed (Non-IID) data [37]. This means the statistical properties of data significantly vary between clients; for instance, clients might hold data with different label distributions (label skew) or different feature characteristics for the same label (feature skew). Such heterogeneity can substantially degrade the performance of standard algorithms like FedAvg, as the single global model aggregated from diverse local models may not generalize well to each client's specific data distribution [7].

2.4. Privacy-Preserving Techniques

FL's privacy benefits can be further enhanced using PETs, with significant advantages and disadvantages, particularly relevant in the resource-constrained IoT context:

Differential Privacy (DP): DP provides a formal, mathematical definition of privacy guarantees [38,39]. A randomized mechanism $\mathcal{M}$ satisfies (ϵ, δ)-DP if, for any two adjacent datasets D_1 and D_2 (differing by at most one element), and for any possible subset of outputs S, the following inequality holds:

$$\mathbb{P}[\mathcal{M}(D_1) \in S] \leq e^{\epsilon}\mathbb{P}[\mathcal{M}(D_2) \in S] + \delta, \tag{2}$$

where ϵ is the privacy budget, and δ represents the probability that the strict ϵ-DP guarantee might be violated. For ϵ, smaller values indicate stronger privacy by limiting the influence of any single data point. For δ, it is typically set to a very small value (e.g., less than the inverse of the dataset size $|D|$). This definition ensures that the output distribution of the mechanism is statistically similar regardless of the presence or absence of any single individual's data [40]. DP guarantees are commonly achieved by adding carefully calibrated noise (e.g., following a Gaussian or Laplace distribution) to function outputs, gradients, or model updates, as implemented in algorithms like DP-SGD [41].

DP offers strong, mathematically rigorous privacy guarantees against inference attacks. Its computational overhead is generally lower compared to cryptographic methods like HE or SMPC. However, a key challenge of DP is the inherent trade-off between privacy and utility, where increasing noise (reducing ϵ) to enhance privacy typically degrades model accuracy [42], as conceptually illustrated in Figure 3. This figure compares the relative computational and communication overheads of various privacy-preserving techniques in FL. It highlights that while DP introduces additional costs, its overhead remains modest compared to more complex methods like SMPC and HE. Notably, homomorphic encryption incurs the highest total overhead, underscoring the practicality of DP in resource-constrained edge scenarios. Managing privacy budgets effectively across rounds and clients is complex [43–45], and DP noise can disproportionately affect fairness for underrepresented groups [3].

 doi:10.20944/preprints202504.2082.v1

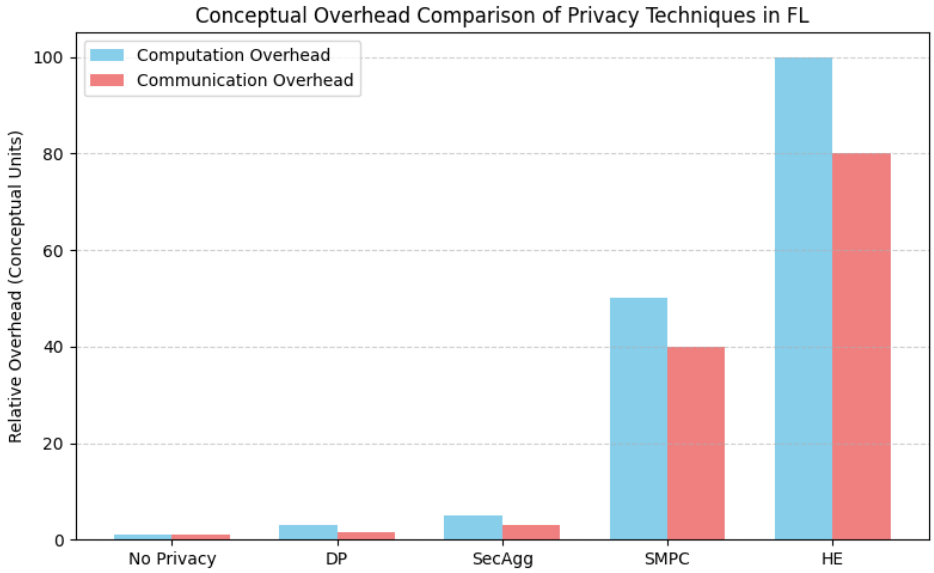

Figure 3. Conceptual illustration of the privacy-utility trade-off in DP. Stronger privacy guarantees (lower ϵ) often correlate with a decrease in model utility or accuracy. The exact curve depends heavily on the dataset, model, and specific DP mechanism.

Homomorphic Encryption (HE): HE allows specific computations (e.g., addition for averaging updates) on encrypted data [46]. The server aggregates ciphertexts without decrypting them. The advantage of HE lies in the fact that it provides strong confidentiality against the server (server learns nothing about individual updates), hence no impact on model accuracy (utility) compared to non-private aggregation. However, HE can have extremely high computational overhead for encryption/decryption and homomorphic operations, significantly expanding the communication data size (ciphertext size). Thus, HE is currently impractical for direct implementation on most resource-constrained IoT devices [7].

Secure Multi-Party Computation (SMPC): SMPC enables multiple parties to jointly compute a function, such as the sum of updates, using cryptographic protocols like secret sharing, without revealing their private inputs [47]. The primary advantage of SMPC lies in its strong privacy guarantees achieved by distributing trust among participants, including potentially the server and clients, with no impact on model accuracy [48]. However, SMPC protocols often require complex multi-round interactions, leading to significant communication overhead. Furthermore, assumptions of synchronous participation or the need for fault tolerance mechanisms add complexity, posing challenges for deployment in dynamic IoT environments [3].

Secure Aggregation: Secure Aggregation utilizes specialized protocols, often based on secret sharing or lightweight cryptography, optimized specifically for the FL aggregation task [49]. These protocols allow the server to securely compute only the sum or average of client updates [50]. Compared to general HE or SMPC, Secure Aggregation is significantly more efficient computationally and communication-wise for this specific task, leading to its widespread adoption in practical FL systems. Nevertheless, while it protects individual updates from the server during the aggregation phase, it does not shield the final aggregated result from potential inference attacks, nor does it secure the updates during transmission unless combined with additional encryption methods.

Table 2 provides a comparative summary of these key privacy-preserving techniques, highlighting their mechanisms, pros, and cons within the FL context. The practical choice often involves secure aggregation, potentially combined with DP for stronger client-level guarantees, or relies on trust in the server, depending heavily on the threat model, system capabilities, and regulatory environment (e.g., GDPR, HIPAA constraints on data processing and transfer) [3,51].

 doi:10.20944/preprints202504.2082.v1

Table 2. Comparison of Key Privacy-Preserving Techniques in the FL Context.

Technique	Mechanism	Pros	Cons
Differential Privacy	Adds calibrated noise to gradients, updates, or data for formal (ϵ, δ) -privacy guarantees.	Strong, mathematical privacy guarantees; relatively lower computational overhead than cryptographic methods.	Direct privacy-utility trade-off (noise vs. accuracy); complex privacy budget management; can impact fairness; overhead can still be significant for resource-poor IoT devices.
Homomorphic Encryption	Allows specific computations (e.g., addition) on encrypted data; server aggregates ciphertexts without decryption.	Strong confidentiality against the server; no impact on model accuracy (utility).	Extremely high computational overhead (encryption, decryption, operations); significant communication overhead (ciphertext size); largely impractical for direct use on most IoT devices.
Secure Multi-Party Computation	Enables joint computation (e.g., sum) via cryptographic protocols without parties revealing private inputs.	Strong privacy guarantees (distributed trust); no impact on model accuracy.	Requires complex multi-round interaction protocols; significant communication overhead; often assumes synchronicity or fault tolerance mechanisms, challenging in dynamic IoT.
Secure Aggregation	Specialized protocols (often secret sharing based) optimized for securely computing the sum/average of client updates.	More efficient (computationally and communication-wise) than general HE/SMPC for the aggregation task; widely adopted.	Protects individual updates from the server *during aggregation*, but not the final aggregated model from inference, nor updates during transmission without extra encryption.

3. LLM-Empowered IoT Architecture for Distributed Systems

3.1. Architectural Overview

Deploying LLMs within IoT often favors multi-tier architectures (Cloud-Edge-Device) to balance computation, latency, and data locality [26]. This involves strategically placing LLM-related tasks: heavy pre-training in the cloud, fine-tuning and inference closer to the edge, and potentially highly optimized inference on capable end devices [25]. This architecture supports both leveraging LLMs for IoT enhancement ("LLM for IoT") and efficiently managing LLMs within IoT constraints ("LLM on IoT") [10].

3.2. LLM for IoT

LLMs can significantly enhance IoT system capabilities through:

- **Intelligent Interfaces & Interaction:** Enabling sophisticated natural language control (e.g., complex conditional commands for smart environments) and dialogue-based interaction with IoT systems for status reporting or troubleshooting [52].
- **Advanced Data Analytics & Reasoning:** Fusing data from multiple sensors (e.g., correlating camera feeds with environmental sensor data for scene understanding in smart cities), performing complex event detection, predicting future states (e.g., equipment failure prediction in IIoT based on subtle degradation patterns), and providing causal explanations for system behavior.
- **Automated Optimization & Control:** Learning complex control policies directly from high-dimensional sensor data for optimizing resource usage (e.g., dynamic energy management in buildings considering real-time occupancy, weather forecasts, and energy prices) or network performance (e.g., adaptive traffic routing in vehicular networks).

3.3. LLM on IoT: Deployment Strategies

Efficiently running LLMs on or near IoT devices requires optimization. In the training stage, model pruning is a typical strategy, while inference adaptation can also be performed for edge devices. These techniques are reviewed next.

 doi:10.20944/preprints202504.2082.v1

3.3.1. Edge Fine-Tuning

Adapting pre-trained models locally using PEFT is key. To adapt large pre-trained models like LLMs without incurring the high computational and memory costs of full fine-tuning, parameter-efficient fine-tuning methods can be employed. A prominent example is the popular LoRA [16]. Instead of updating the entire pre-trained weight matrix $\mathbf{W}_0 \in \mathbb{R}^{d\times k}$, LoRA introduces two smaller, low-rank matrices, $\mathbf{A} \in \mathbb{R}^{d\times r}$ and $\mathbf{B} \in \mathbb{R}^{r\times k}$, where the rank r is typically much smaller than d or k (i.e., $r \ll \min(d,k)$). The core idea is to represent the weight update $\Delta\mathbf{W}$ as the product of these low-rank matrices ($\Delta\mathbf{W} = \mathbf{BA}$). During fine-tuning, the original weights $\mathbf{W}_0$ remain frozen, and only the parameters in $\mathbf{A}$ and $\mathbf{B}$ are trained. This mechanism is illustrated in Figure 4. The effective weight matrix used in the forward pass is then computed as:

$$\mathbf{W} = \mathbf{W}_0 + \Delta\mathbf{W} = \mathbf{W}_0 + \mathbf{BA}. \tag{3}$$

This approach drastically reduces the number of trainable parameters from $d \times k$ for full fine-tuning down to only $r \times (d + k)$ for LoRA [53]. This significant reduction in parameters, memory usage, and computation makes fine-tuning large models feasible even on resource-constrained edge devices and substantially decreases communication overhead in federated learning scenarios where only the small $\mathbf{A}$ and $\mathbf{B}$ matrices need to be exchanged [54].

However, PEFT methods like LoRA involve benefits and drawbacks. The choice of the rank r directly impacts the balance between efficiency and the model's adaptation capacity; a very low rank might limit the model's ability to capture complex task-specific nuances [55]. Furthermore, the generalization capability of PEFT methods, especially when adapting models to tasks significantly different from the pre-training data, compared to full fine-tuning, remains an active area of investigation [56].

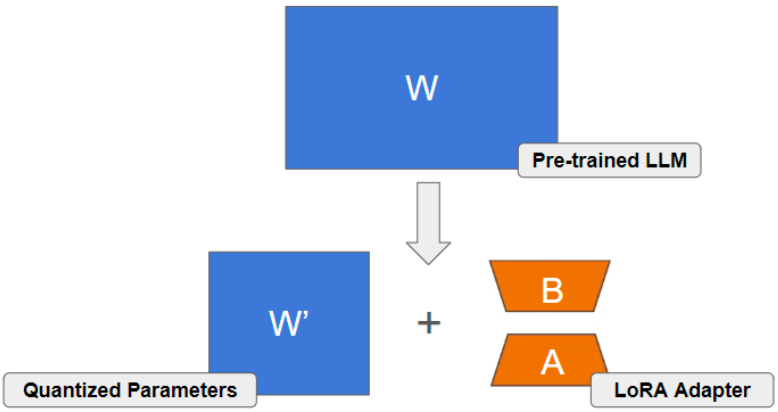

Figure 4. Illustration of the LoRA adapter mechanism, potentially used with quantized base model weights (as in QLoRA [57]). The large pre-trained weights (W) might be stored in a quantized format (W'), while the task-specific update is learned via the small, trainable low-rank adapter matrices (B and A).

3.3.2. Edge Inference

Prediction/generation performance can be optimized through the following techniques.

- **On-device Inference:** Utilizes model compression (Quantization, Pruning, Distillation) [57,58]. Compression inherently risks degrading model accuracy or robustness; and the extent depends heavily on the technique and compression ratio [59].
- **Co-inference / Split Inference:** Divides layers between device and edge server [18]. It introduces network latency and dependency on the edge server, although keeps raw data local. This is distinct from SFL used for training.
- **Edge Caching:** Reduces latency for repeated queries [3].

 doi:10.20944/preprints202504.2082.v1

4. Federated Learning for Privacy-Preserving LLM Training in IoT

Having established the foundational concepts and architectural considerations, this section delves into the specific methodologies required to effectively train and adapt LLMs within distributed IoT environments using FL. We examine various techniques designed to overcome the inherent challenges of resource constraints, communication overhead, data heterogeneity, and privacy concerns that arise when integrating these powerful models with FL paradigms at the edge [54]. Key topics include core federated fine-tuning strategies tailored for LLMs, methods for personalization, alternative training approaches, essential supporting frameworks and data handling techniques, the emerging role of LLMs in aiding the FL process itself, and crucial evaluation metrics specific to this context [60]. Understanding these methodologies is crucial for realizing the practical potential of the synergistic IoT, LLM, and FL integration.

4.1. Federated Fine-Tuning of LLMs

Applying FL to fine-tune Large Language Models enables collaborative adaptation on decentralized IoT data, crucial for personalization and domain specialization while preserving privacy [23]. The integration of FL with PEFT methods, particularly LoRA, significantly reduces communication overhead by transmitting only lightweight parameter updates (typically <1% of total model parameters) [61]. Beyond CFL approaches, research is exploring decentralized fine-tuning methods [62]. For instance, Dec-LoRA is an algorithm designed for decentralized fine-tuning of LLMs using LoRA without relying on a central parameter server [63]. Experimental results suggest that Dec-LoRA can achieve performance comparable to centralized LoRA, even when facing challenges like data heterogeneity and quantization constraints, offering a potential pathway for more robust and scalable federated fine-tuning in certain network topologies [53].

4.2. Split Federated Learning

SFL addresses the critical memory limitations on edge devices during the training phase of large models within an FL context [19]. By partitioning the model and offloading a significant portion of the computation (especially backward passes through deeper layers) to a server, SFL allows memory-constrained devices to participate [18]. Integrating LoRA further optimizes this [17]. However, SFL introduces latency due to the necessary exchange of activations and gradients between client and server per iteration; and its performance is sensitive to the network bandwidth and the choice of the model split point [18].

4.3. Personalized Federated LLMs (PFL)

PFL methods are vital for addressing client heterogeneity in FL, aiming to provide models better suited to individual client data or capabilities than a single global model [64,65]. Table 3 provides a comparative overview.

4.4. Back-Propagation-Free Methods

These methods (e.g., zeroth-order optimization) bypass standard backpropagation, reducing peak memory usage by eliminating the need to store activations [78–81]. Limitations: They often require significantly more function evaluations (slower convergence) and can be less stable or scalable for very high-dimensional parameter spaces compared to gradient-based methods [78,82]. Their practical application in large-scale federated LLM training remains an active research topic.

4.5. Frameworks and Benchmarks

The practical implementation and evaluation of federated LLMs rely on specialized software frameworks and benchmarks:

Frameworks: Libraries like FedML [83] with its FedLLM component [83], Flower [84,85], FATE-LLM [86], and FederatedScope-LLM [87] provide infrastructure for simulating or deploying FL. Features relevant to IoT/edge include support for heterogeneous devices, PEFT methods (e.g., LoRA),

 doi:10.20944/preprints202504.2082.v1

Table 3. Comparative Overview of Personalized PFL Approaches for LLMs.

Approach	Mechanism	Heterogeneity Handled	Efficiency	Trade-offs
PEFT-based PFL (Prompts, Adapters, LoRA)	Clients train personalized PEFT components attached to a shared, frozen LLM backbone. Global aggregation might occur on these PEFT components or parts thereof [16,54,66–68].	Primarily statistical (data); some methods adapt to system heterogeneity by adjusting PEFT complexity (e.g., heterogeneous LoRA ranks) [69,70].	High communication efficiency (small updates); moderate computation (only PEFT tuning) [71].	Personalization depth limited by PEFT capacity; potential for negative interference if global components are poorly aggregated [72].
Model Decomposition / Partial Training	Global model is structurally divided; clients train only specific assigned layers or blocks [60, 73,74].	Primarily system (computation/memory); can assign smaller parts to weaker clients.	Reduced client computation; communication depends on the size of trained part.	Less flexible personalization compared to PEFT; requires careful model partitioning design; potential information loss between components.
Knowledge Distillation (KD) based PFL	Uses outputs (logits) or intermediate features from a global "teacher" model (or ensemble of client models) to guide the training of personalized local "student" models [75–77].	Can handle model heterogeneity (different student architectures); adaptable to data heterogeneity.	Communication involves logits/features, potentially smaller than parameters; client computation depends on student model size.	Distillation process can be complex; potential privacy leakage from shared logits; the student's model might not perfectly capture the teacher's knowledge.
Meta-Learning based PFL (e.g., Reptile, MAML adaptations)	Learns a global model initialization that can be rapidly adapted (fine-tuned) to each client's local data with few gradient steps [65].	Focuses on adapting to statistical (data) heterogeneity.	Communication similar to standard FL; potentially more local computation during adaptation phase.	Can be sensitive to task diversity across clients; training the meta-model can be computationally intensive.

various aggregation algorithms, security mechanisms (DP, secure aggregation), and sometimes specific optimizations for edge deployment (e.g., efficient client runtimes, handling intermittent connectivity). Selecting a framework depends on the specific research or deployment needs regarding scale, flexibility, supported models, and available privacy/security features.

Benchmarks: Standardized datasets and evaluation protocols are crucial for comparing different algorithms. Efforts like FedIT [88] focus on benchmarking federated instruction tuning. FedNLP [89] provided early benchmarks for standard NLP tasks in FL. OpenFedLLM aims to offer a comprehensive platform with multiple datasets and metrics [90]. However, benchmarks specifically capturing the complexities of real-world IoT data heterogeneity, network conditions, and device constraints for LLMs are still needed.

4.6. Initialization and Data Considerations

Effective federated LLM training depends significantly on model initialization and data handling:

Model Initialization: Starting FL from a well-pre-trained LLM, rather than random initialization, significantly improves convergence speed, final model performance, and robustness to non-IID data [91]. It allows FL to focus on adaptation rather than learning foundational knowledge from scratch [92].

Data Processing: Handling massive, distributed datasets requires scalable tools. Libraries like Dataset Grouper aim to facilitate partitioning large datasets for FL simulation [93].

 doi:10.20944/preprints202504.2082.v1

Synthetic Data Generation: When local data is scarce or highly skewed, generating synthetic data can augment training [10]. LLMs themselves show promise for generating high-quality synthetic data that reflects complex real-world distributions, potentially overcoming limitations of earlier generative models used in FL [94]. Frameworks like GPT-FL explore using LLM-generated data to aid FL. Selecting relevant public data using distribution matching techniques can also enhance privacy-preserving training via knowledge distillation [95].

4.7. LLM-Assisted Federated Learning

Beyond using FL to train LLMs, the reciprocal relationship where LLMs assist FL is also emerging [23]:

Mitigating Data Heterogeneity: LLMs pre-trained on vast datasets can generate high-quality synthetic data reflecting diverse distributions. This synthetic data can be used centrally or shared (with privacy considerations) to augment clients' local datasets, helping to alleviate the negative impacts of non-IID data on FL convergence [94].

Knowledge Distillation: A large, powerful LLM (potentially centrally available or trained via FL itself) can act as a "teacher" model. Its knowledge (e.g., predictions, representations) can be distilled into smaller "student" models trained by clients in the FL network, improving the efficiency and performance of client models, especially on resource-constrained devices [55].

Intelligent FL Orchestration: LLMs could potentially be used for more sophisticated FL management tasks, such as predicting client resource availability, assessing data quality for client selection, or even dynamically tuning FL hyperparameters based on observed training dynamics.

4.8. Evaluation Metrics

Evaluating federated LLM systems requires a multi-faceted approach beyond standard accuracy measures, particularly in the IoT context (See Table 4). Developing standardized benchmarks that allow for consistent evaluation across these diverse metrics is a key challenge and future direction [88]. Table 4 summarises the key categories of evaluation, including model utility, efficiency, privacy, fairness, and scalability, each with specific metrics tailored to the constraints and demands of federated IoT settings. For instance, communication and computation efficiency metrics reflect the limited bandwidth, energy, and processing power typical of edge devices. Privacy is evaluated through both theoretical guarantees (such as differential privacy parameters) and empirical attack resistance, while fairness and scalability ensure inclusiveness and robustness across heterogeneous clients. Together, these metrics offer a comprehensive framework for assessing the real-world feasibility and trustworthiness of federated LLM systems deployed across diverse and distributed IoT environments.

5. Synergistic Effects of Integrating IoT, LLMs, and Federated Learning

5.1. Introduction: Beyond Pairwise Integration

The previous sections have laid the groundwork by introducing the core concepts and individual capabilities of the Internet of Things [24], Large Language Models [27], and FL [9]. While pairwise integrations – such as applying LLMs to IoT data analytics [96], using FL for privacy-preserving IoT applications [20,21], or employing FL to train LLMs [23], offer significant advancements, they often encounter inherent limitations [10]. Centralized LLM processing of IoT data raises critical privacy and communication bottlenecks [13]; traditional FL models struggle with the complexity and scale of raw IoT data [14]; and federated LLMs without direct access to real-world IoT streams lack crucial grounding and context [7].

This section argues that the true transformative potential lies in the *synergistic convergence of all three technologies: IoT, LLMs, and FL*, explicitly enhanced by Privacy-Enhancing Technologies [42]. This three-way integration creates a powerful ecosystem where the strengths of each component compensate for the weaknesses of the others, enabling capabilities and solutions that are fundamentally unattainable or significantly less effective otherwise [38]. We posit that this synergy is not merely additive but

 doi:10.20944/preprints202504.2082.v1

Table 4. Key Evaluation Metrics for Federated LLM Systems in IoT Contexts.

Category	Specific Metrics Examples	Relevance/Notes
Model Utility	Accuracy, F1-score, BLEU, ROUGE, Perplexity, Calibration, Robustness (to noise, adversarial inputs)	Task-specific performance and reliability of the learned model.
Efficiency:		Crucial for resource-constrained and bandwidth-limited IoT environments.
- *Communication*	Total bytes/bits transmitted, Number of rounds, Compression rates	Impacts network load, energy consumption on wireless devices.
- *Computation*	Client training time/round, Server aggregation time, Edge inference latency, Total FLOPs, Energy consumption	Determines feasibility on device, overall system speed, battery life.
- *Memory*	Peak RAM usage (client/server), Model storage size	Critical for devices with limited memory capacity.
Privacy	Formal guarantees (e.g., (ϵ, δ) -DP values), Empirical leakage (e.g., Membership Inference Attack success rate)	Quantifies the level of privacy protection provided against specific threats.
Fairness	Variance in accuracy across clients/groups, Worst-group performance vs. average	Measures consistency of performance for diverse participants or data subpopulations.
Scalability	Performance/efficiency degradation as the number of clients increases	Assesses the system's ability to handle large-scale IoT deployments.

multiplicative, paving the way for a new generation of advanced, privacy-preserving, context-aware distributed intelligence operating directly at the network edge [15]. We will explore this "1+1+1 > 3" effect through three core synergistic themes, building upon the motivations discussed in works like [49].

5.2. Theme 1: Privacy-Preserving, Context-Aware Intelligence from Distributed Real-World Data

The Challenge: LLMs thrive on vast, diverse, and timely data to develop nuanced understanding and maintain relevance [8]. IoT environments generate precisely this type of data – rich, real-time, multi-modal streams reflecting the complexities of the physical world [7,42]. However, this data is inherently distributed across countless devices and locations [14], and often contains highly sensitive personal, operational, or commercial information, making centralized collection legally problematic (e.g., GDPR, HIPAA compliance [21]), technically challenging (bandwidth costs, latency [13]), and ethically undesirable [5,22]. Relying solely on public datasets limits LLM grounding and domain specificity [10].

The Synergy (IoT + LLM + FL): Federated Learning acts as the crucial *enabling mechanism* [9] that allows LLMs to tap into the rich, distributed data streams generated by IoT devices *without compromising data locality and privacy* [15]. IoT provides the continuous flow of real-world, multi-modal data (the "what" and "where") [14]. FL provides the privacy-preserving framework for collaborative learning across these distributed sources (the "how") [10]. The LLM provides the advanced cognitive capabilities to learn deep representations, understand context, and extract meaningful intelligence from this data (the "why" and "so what?") [60].

Emergent Capability: This synergy empowers LLMs to maintain robust general capabilities while dynamically adapting to specific real-world contexts. By leveraging fresh, diverse, and privacy-sensitive IoT data, these models achieve continuous grounding in evolving environments. This allows for:

- *Hyper-Personalization:* Training models tailored to individual users or specific environments (e.g., a smart home assistant learning user routines from sensor data via FL [14]).

 doi:10.20944/preprints202504.2082.v1

- *Real-time Domain Adaptation:* Continuously fine-tuning LLMs (e.g., using PEFT like LoRA [54]) with the latest IoT data to adapt to changing conditions (e.g., adapting a traffic prediction LLM based on real-time sensor feeds from different city zones [97]).
- *Enhanced Robustness:* Learning from diverse, real-world IoT data sources via FL can make LLMs more robust to noise and domain shifts compared to training solely on cleaner, but potentially less representative, centralized datasets [37].

5.3. Theme 2: Intelligent Interpretation and Action Within Complex IoT Environments

The Challenge: IoT environments produce data that is often complex, noisy, unstructured, and multi-modal (e.g., raw sensor time-series, machine logs, video feeds, acoustic signals) [14]. Traditional FL, while preserving privacy, often employs simpler models that struggle to extract deep semantic meaning or perform complex reasoning on such data [42]. Conversely, powerful LLMs, while capable of understanding complexity [15], lack the direct connection to the physical world for sensing and actuation and struggle with distributed private data access [98].

The Synergy (IoT + LLM + FL): LLMs bring sophisticated *natural language understanding, reasoning, and generation capabilities* to the table [1], allowing the system to interpret intricate patterns, correlate information across different IoT modalities, and even generate human-readable explanations or reports [96]. FL provides the means to *train these powerful LLMs collaboratively* using the relevant complex IoT data distributed across the network [54]. Crucially, IoT devices provide the *physical grounding*, acting as the sensors collecting the complex data and potentially as actuators executing decisions derived from LLM insights [3]. Furthermore, LLMs can enhance the FL process itself by intelligently guiding client selection based on interpreting the relevance or quality of their IoT data, or even assisting in designing personalized FL strategies [15].

Emergent Capability: The combination allows for systems that can *deeply understand complex physical environments and interact intelligently within them*. This goes beyond simple data aggregation or pattern matching:

Contextual Anomaly Detection: Identifying subtle anomalies in IIoT machine behavior by correlating multi-sensor data and unstructured logs, understood and explained by an LLM trained via FL [99]. *Causal Reasoning in Smart Cities:* Using FL-trained LLMs to analyze diverse IoT data (traffic, pollution, events) to infer causal relationships and predict cascading effects [14,97]. *Goal-Oriented Dialogue with Physical Systems:* Enabling users to interact with complex IoT environments (e.g., a smart factory floor) using natural language, where an LLM interprets the request, queries relevant IoT data (potentially involving FL for aggregation), and generates responses or even commands for actuators [15].

5.4. Theme 3: Scalable and Adaptive Domain Specialization at the Edge

The Challenge: Deploying large, general-purpose LLMs directly onto resource-constrained IoT devices is often infeasible due to their size and computational requirements [57]. While smaller, specialized models can run on the edge, training them from scratch for every specific IoT application or location is inefficient and doesn't leverage the power of large pre-trained models [15]. Centralized fine-tuning of large models for specific domains requires access to potentially private or distributed IoT data [13].

The Synergy (IoT + LLM + FL): FL combined with *PEFT* techniques like LoRA [61] provides a highly *scalable and resource-efficient* way to specialize pre-trained LLMs for diverse IoT domains using distributed edge data [13,53]. IoT devices/edge servers provide the specific local data needed for adaptation [14]. PEFT ensures that only a small fraction of parameters need to be trained and communicated during the FL process, drastically reducing computation and communication overhead [54,73]. The base LLM provides the powerful foundational knowledge, while FL+PEFT enables distributed, privacy-preserving specialization [62].

Emergent Capability: This synergy enables the *mass customization and deployment of powerful, specialized AI capabilities directly within diverse IoT environments*. Key outcomes include:

 doi:10.20944/preprints202504.2082.v1

- *Locally Optimized Performance:* Models fine-tuned via FL+PEFT on local IoT data will likely outperform generic models for specific edge tasks (e.g., a traffic sign recognition LLM adapted via FL to local signage variations [14]).
- *Rapid Adaptation:* New IoT devices or locations can quickly join the FL process and adapt the shared base LLM using PEFT without needing massive data transfers or full retraining [10].
- *Resource-Aware Deployment:* Allows leveraging powerful base LLMs even when end devices can only handle the computation for small PEFT updates during FL training [70], or optimized inference models (potentially distilled using FL-trained knowledge [77]). Frameworks like Split Federated Learning can further distribute the load [17,18].

5.5. Illustrative Use Case: Predictive Maintenance in Federated Industrial IoT (IIoT)

Consider a scenario involving multiple manufacturing plants belonging to different subsidiaries of a large corporation, or even different collaborating companies [99]. Each plant operates similar types of critical machinery (e.g., CNC machines, robotic arms) equipped with various sensors (vibration, temperature, acoustic, power consumption - the IoT component). The goal is to predict potential machine failures proactively across the entire fleet to minimize downtime and optimize maintenance schedules, while ensuring that proprietary operational data and specific machine performance characteristics from one plant are not shared with others.

Below, we summarize the limitations without synergy.

- *IoT only:* Basic thresholding or simple local models on sensor data might miss complex failure patterns. No collaborative learning.
- *IoT + Cloud LLM:* Requires sending massive, potentially sensitive sensor streams and logs to the cloud, incurring high costs, latency, and privacy risks [13].
- *IoT + FL (Simple Models):* Can learn collaboratively but struggles to interpret unstructured maintenance logs or complex multi-sensor correlations indicative of subtle wear patterns [14].
- *LLM + FL (No IoT):* Lacks real-time grounding; trained on potentially outdated or generic data, not the specific, current state of the machines [10].

To address the issues highlighted above, a synergistic solution (IoT + LLM + FL) is illustrated next.

- **Data Generation :** Sensors on machines continuously generate multi-modal time-series data and operational logs.
- **Model Choice (LLM):** A powerful foundation LLM (potentially pre-trained on general engineering texts and machine manuals) is chosen as the base model. It possesses the capability to understand technical language in logs and potentially process time-series data patterns [15].
- **Collaborative Fine-Tuning (FL + PEFT):** FL is used to fine-tune this LLM across the plants using their local IoT sensor data and maintenance logs [60]. To manage resources and communication, PEFT (e.g., LoRA [16]) is employed. Only the small LoRA adapter updates are shared with a central FL server (or aggregated decentrally [63]) – preserving privacy regarding raw data and detailed operational parameters [54].
- **Intelligence & Action (LLM + IoT):** The fine-tuned LLM (potentially deployed at edge servers within each plant [13]) analyzes incoming IoT data streams and logs in near real-time. It identifies complex failure precursors missed by simpler models, correlates sensor data with log entries, predicts remaining useful life, and generates concise, human-readable alerts and maintenance recommendations for specific machines [99]. These alerts can be directly integrated into the plant's maintenance workflow system (potentially an IoT actuation).

This integrated system can achieve highly accurate, context-aware predictive maintenance across multiple entities by leveraging diverse operational data (IoT) through privacy-preserving collaborative learning (FL), powered by the deep analytical and interpretive capabilities of LLMs, all achieved efficiently using PEFT. This outcome would be significantly harder, if not impossible, to achieve with only two of the three components.

 doi:10.20944/preprints202504.2082.v1

5.6. Challenges Arising from the Synergy

While powerful, the tight integration of IoT, LLMs, and FL introduces unique challenges beyond those of the individual components:

Cross-Domain Data Alignment & Fusion: Effectively aligning and fusing heterogeneous, multi-modal IoT data streams within an FL framework *before* feeding them to an LLM requires sophisticated alignment and representation techniques [96].

Resource Allocation Complexity: How to jointly optimize computation (LLM inference/training, FL aggregation), communication (IoT data upload, FL updates), and privacy (PET overhead) across heterogeneous IoT devices, edge servers, and potentially the cloud specifically for this integrated task [13]?

Model Synchronization vs. Real-time Needs: Balancing the need for FL model synchronization (potentially slow for large LLM updates [10]) with the real-time data processing and decision-making requirements of many IoT applications.

Emergent Security Vulnerabilities: New attack surfaces emerge at the interfaces, e.g., malicious IoT data poisoning FL training *specifically to mislead the LLM's interpretation* [100], or FL privacy attacks aiming to reconstruct sensitive IoT context interpreted by the LLM [101]. Verifying the integrity of both IoT data and FL updates becomes critical [15].

5.7. Concluding Remarks on Synergy

The convergence of IoT, Large Language Models, and Federated Learning represents a fundamental paradigm shift in designing intelligent distributed systems. As demonstrated, their synergy unlocks capabilities far exceeding the sum of their individual parts. By enabling powerful LLMs to learn from diverse, real-world, privacy-sensitive IoT data through the secure framework of FL, we can create adaptive, context-aware, and specialized AI solutions deployable at the network edge. This synergy directly addresses the limitations inherent in previous approaches, paving the way for truly intelligent, efficient, and trustworthy applications across critical domains like Industrial IoT, autonomous systems, and smart infrastructure. While unique challenges arise from this tight integration, they also define fertile ground for future research focused on realizing the full, transformative potential of this powerful technological triad.

6. Key Challenges and Mitigation Strategies

In this section, we identify the key challenges of the synergy of IoT, LLM, and FL, and suggest potential mitigation strategies based on relevant techniques found in the open literature. Table 5 summarises the main challenges and mitigation methods, as elaborated on next.

6.1. Resource Constraints

A primary obstacle when deploying LLMs within IoT ecosystems arises from the stark mismatch between the models' demands and the typically severe resource constraints of edge devices [3]. Edge units often provide limited processing power, small memory capacities (e.g., typically 1–4 GB of RAM), and must operate under strict power budgets (often $\leq$ 10 W) [24]. Yet, even moderately sized models, like a 7 billion-parameter LLM, can require approximately 4 GB of memory just for inference, making deployment challenging [10].

To bridge this gap and enable on-device LLM adaptation and execution, several mitigation strategies focusing on efficiency can be employed. Model Compression techniques, notably quantization (e.g., to 4-bit precision), can significantly slash memory usage by roughly 75% while often preserving a high percentage (e.g., 92–97%) of the original model's accuracy on tasks like text classification [57]. Another approach is Split Computing, particularly SFL, which partitions the model layers between the device and a more capable edge server. This can cut on-device memory requirements substantially (e.g., by 40–60%), though it introduces trade-offs such as increased round-trip latency (e.g., 150–300 ms) during operations like federated training iterations [18]. Furthermore, PEFT methods have emerged

 doi:10.20944/preprints202504.2082.v1

Table 5. Major Challenges in Integrating IoT, LLMs, and FL, with Mitigation Strategies.

Challenge	Description	Mitigation Strategies	Trade-offs / Notes
Resource Constraints (Compute, Memory, Energy)	Severe limitations on many IoT devices conflict with LLM computational demands [3,24].	Model Compression [57]; Split Computing [3,18]; PEFT [16]; Adaptive Distribution.	Accuracy loss (Compression); Latency/Sync needs (Split); Limited adaptivity ; Orchestration complexity (Adaptive).
Communication Overhead	High cost of transmitting large model updates frequently over constrained IoT networks [10,102].	PEFT [16]; Update Compression [102]; Reduced Frequency [9]; Asynchronous Protocols [92,103].	Smaller updates limit model changes ; Info loss risk (Compression); Slower convergence (Frequency); Staleness issues (Async).
Data Heterogeneity (Non-IID) & Fairness	Non-IID data hinders convergence and fairness [37,104]; biases can be amplified [30]; decentralized bias mitigation is hard.	Robust Aggregation (e.g., FedProx) [37]; PFL [64,65]; Fairness-aware Algorithms; Synthetic/Public Data Augmentation [94,95].	Complexity (PFL); Potential avg. accuracy reduction (Fairness); Privacy concerns with data augmentation.
Privacy & Security Risks	Balancing privacy vs. utility; protecting against leakage [101,105], poisoning [100,106], Byzantine [107], backdoor attacks [108–110]; regulatory compliance (GDPR, HIPAA).	PETs (DP [41], HE [46], SMPC [48], Secure Aggregation [49]); Robust Aggregation (e.g., Krum [107], PEAR [111]); Attack Detection [112,113]; TEEs [114]; ZKP-based methods (e.g., ByzSFL [115]).	Accuracy loss (DP) [42]; High overhead (HE/SMPC) [3]; Limited protection (SecAgg); Assumptions fail (Robust Agg.); Verifiability (ZKP). See Table 2.
On-Demand Deployment & Scalability	Efficiently managing FL training and LLM inference across massive, dynamic IoT populations [3].	Edge Infrastructure Optimization (Caching, Serving) [3]; Scalable FL Orchestration (Hierarchical, Decentralized, Asynchronous) [35,92,116]; Resource-Aware Management [3,36].	Orchestration trade-offs; Incentive complexity.

as a highly promising strategy. Techniques like LoRA drastically reduce the number of trainable parameters by updating only a small fraction (e.g., about 1–2%) of the model's weights, achieving massive reductions (up to 98%) in parameters needing training and storage [16]. Impressively, this efficiency often comes with only a modest decrease in performance, retaining substantial percentages (e.g., around 89%) of full fine-tuning performance on standard benchmarks.

Full fine-tuning involves updating all model parameters, which leads to the highest performance but at a substantial computational and memory cost. In contrast, PEFT methods significantly reduce the number of trainable parameters—LoRA updates approximately 1% of parameters, Adapters around 2%, and Prompt-Tuning fewer than 0.1%—while still achieving competitive downstream task performance. As the figure illustrates, these methods strike different balances between efficiency and effectiveness, making them particularly attractive for resource-constrained IoT and federated learning settings where full fine-tuning is often impractical. This visual comparison underscores the growing importance of PEFT techniques in scaling LLM applications to diverse, decentralized edge environments.

The trade-offs between parameter efficiency and task performance for various PEFT methods, including LoRA, Adapter tuning, and Prompt-tuning compared to Full Fine-tuning, are clearly visualized in Figure 5.

 doi:10.20944/preprints202504.2082.v1

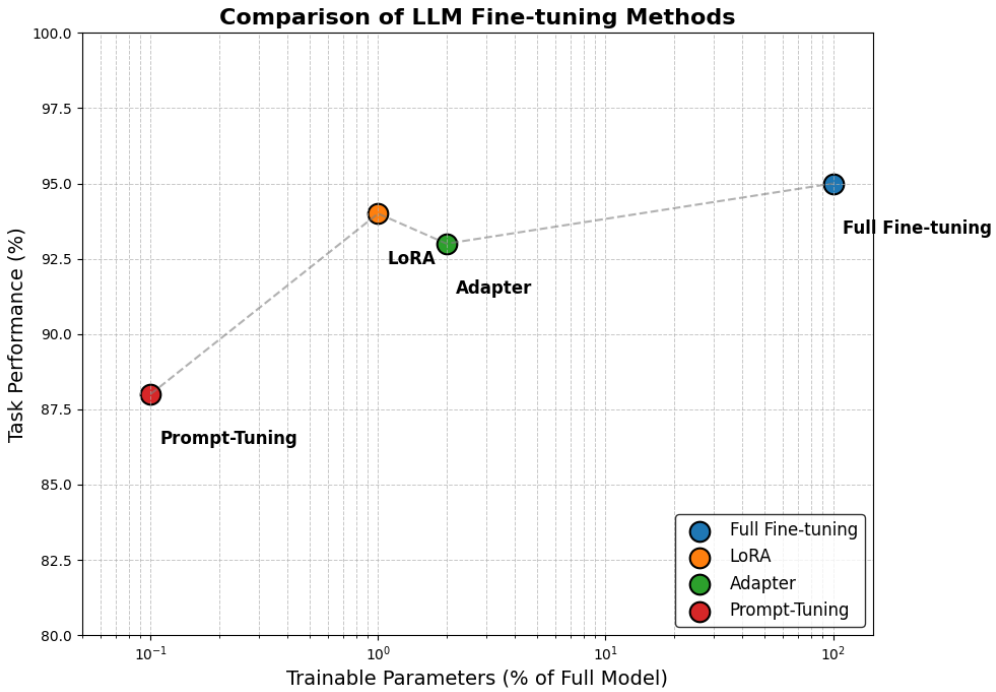

Figure 5. Trade-off between trainable parameter ratio and downstream task performance for various LLM fine-tuning methods. Full fine-tuning updates 100% of parameters, whereas PEFT approaches such as LoRA (1%), Adapter (2%), and Prompt-Tuning (<0.1%) offer large savings in parameter updates at the cost of some performance.

Finally, complementing these model-level optimizations, adaptive distribution techniques employing dynamic workload schedulers can monitor real-time device telemetry (available RAM, CPU load, network bandwidth) to adjust model partitioning or batch sizes on-the-fly, maximizing the utilization of available resources. Together, these diverse approaches—compression, splitting, parameter-efficient adaptation, and dynamic scheduling—make it increasingly practical to deploy and adapt sophisticated LLMs effectively on resource-constrained IoT hardware.

6.2. Communication Overhead

The high communication overhead associated with FL poses another significant challenge, particularly in IoT networks characterized by potentially unreliable or low-bandwidth connections [10]. Transmitting large model updates frequently between numerous devices and a central server can saturate the network and consume considerable energy. Several approaches aim to mitigate this communication burden. As mentioned, PEFT methods are highly effective, as only the small adapter updates need to be transmitted [92]. Update Compression techniques can further reduce the size of transmitted data, but carry a risk of information loss [102]. Reducing the frequency of communication rounds can save bandwidth, but typically slows down the convergence of the global model [9]. Additionally, Asynchronous Protocols allow devices to communicate more flexibly based on their availability, alleviating delays caused by stragglers, but they introduce challenges related to model staleness and potential inconsistencies [103].

6.3. Data Heterogeneity and Fairness

The performance and fairness of FL systems are significantly impacted by data heterogeneity, commonly referred to as Non-IID data, which is prevalent in IoT environments [104]. Data distributions often vary substantially across devices due to differing local environments, usage patterns, or sensor types (e.g., label or feature skew). This heterogeneity can hinder the convergence of standard FL algorithms like FedAvg and lead to a global model that performs poorly for specific clients. Furthermore, biases present in local data or even within the pre-trained base LLM can be amplified or unfairly

 doi:10.20944/preprints202504.2082.v1

distributed across participants through the FL process, and measuring or mitigating such biases in a decentralized manner remains difficult [30]. Strategies to address Non-IID data and promote fairness include using Robust Aggregation algorithms (like FedProx) designed to be less sensitive to diverging updates [37], and employing PFL techniques that tailor parts of the model to local data, although this adds complexity [64,65]. Fairness-aware algorithms explicitly try to balance performance across different client groups, sometimes at the cost of overall average accuracy. Another approach involves augmenting local data with synthetic data (potentially generated by LLMs) or relevant public data, but this requires careful consideration of privacy implications [94,95].

6.4. Privacy and Security Risks

Ensuring robust privacy and security is perhaps the most critical challenge, given the sensitive nature of IoT data and the distributed nature of FL. Key concerns involve balancing model utility against privacy guarantees, protecting against various attacks such as data leakage from model updates [101,105], data or model poisoning by malicious clients [100,106], Byzantine failures [107], and backdoor attacks targeting the models [108–110], all while complying with regulatory mandates like GDPR or HIPAA.

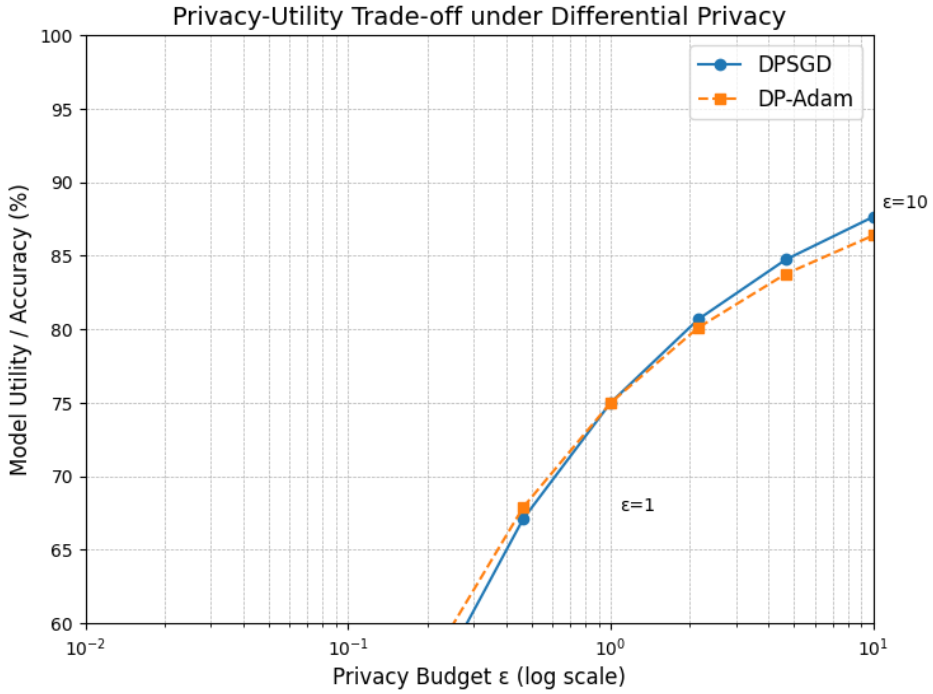

Figure 6. Illustration of the privacy-utility trade-off under differential privacy for federated learning models. The plot compares the model accuracy (%) of two different DP-based optimization methods, DPSGD and DP-Adam, across a range of privacy budgets (ϵ) on a logarithmic scale. As the privacy guarantee strengthens (smaller ϵ), model performance consistently degrades, highlighting the inherent trade-off between privacy protection and predictive utility. Key privacy levels (ϵ = 0.01, 0.1, 1, and 10) are annotated to demonstrate performance sensitivity.

A variety of techniques, often referred to as PETs and robust mechanisms, are used to mitigate these risks, each with distinct trade-offs in aspects like overhead (conceptually compared in Figure 6) and utility. DP offers strong, mathematical guarantees against inference attacks by adding calibrated noise. While generally having lower computational overhead than cryptographic methods, it introduces a direct privacy-utility trade-off, where increasing noise to enhance privacy typically degrades model accuracy [42], as illustrated conceptually in Figure 6. Cryptographic approaches like HE allow computations (like aggregation) on encrypted data, providing strong confidentiality against the server without accuracy loss, but their extremely high computational and communication overhead makes them largely impractical for direct use on most IoT clients [3,46]. Similarly, SMPC enables joint compu-

 doi:10.20944/preprints202504.2082.v1

tations without revealing private inputs, offering strong security through distributed trust with no accuracy loss, but typically requires complex, multi-round interactions unsuitable for dynamic IoT environments [48]. Secure aggregation protocols are optimized specifically for the FL summation task, offering much better efficiency than general HE/SMPC and protecting individual updates from the server during aggregation, but they do not protect the final model from inference or updates during transmission without additional measures [49].

To defend against malicious clients sending faulty updates (poisoning or Byzantine attacks), Robust aggregation methods like Krum [107], Bulyan [117], coordinate-wise median, or trimmed mean are employed to filter outlier updates. However, their effectiveness can decrease with sophisticated attacks or high Non-IID levels [118,119]. Recent advancements show promise, such as the PEAR mechanism using cosine similarity and trust scores for better robustness in Non-IID settings [111], or techniques like ByzSFL that integrate Byzantine robustness with secure computation using Zero-Knowledge Proofs (ZKPs) for efficient verification without revealing private data [115]. Complementary strategies include explicit attack detection and verification mechanisms [112,113] and leveraging hardware security through Trusted Execution Environments (TEEs) to provide protected enclaves for computation [114].

6.5. Scalability and On-Demand Deployment

Finally, achieving efficient scalability and supporting on-demand deployment is crucial for applying FL-trained LLMs across massive and dynamic IoT populations [35]. Managing the training process and subsequent inference efficiently requires optimized edge infrastructure, including techniques like caching and optimized model serving [36]. Scalable FL orchestration is also essential, employing architectures like Hierarchical, Decentralized, or Asynchronous FL, each presenting different trade-offs in coordination complexity, robustness to failures or stragglers, and communication latency [92]. Furthermore, effective Resource-aware management, incorporating adaptive scheduling, intelligent client selection strategies, and potentially incentive mechanisms, is needed to handle the dynamic nature of device availability and network conditions [116].

7. Research Gaps and Future Directions

Despite rapid progress, the integration of IoT, LLMs, and FL still faces substantial challenges. This section identifies critical research gaps, with detailed evidence and insights from recent literature.

Efficiency for Extreme Edge: LLMs are notoriously resource-intensive, but edge IoT devices often operate on milliwatts of power with kilobytes of RAM. Techniques like QLoRA [57] reduce fine-tuning memory use by combining 4-bit quantisation and low-rank adaptation, making LLMs tractable for edge execution. Similarly, SparseGPT achieves one-shot pruning with negligible accuracy drop on billion-parameter models [58]. SmoothQuant enhances post-training quantisation by aligning activations and weights to improve stability under int8 quantisation [59]. Backpropagation-free training is emerging as a potential direction to eliminate memory-heavy gradient calculations; the survey in [78] reviews biologically inspired and forward-forward alternatives relevant to constrained hardware. These are particularly promising when combined with hardware-aware co-design, as advocated in [3], for FL in 6G IoT networks.

Robustness to Heterogeneity and Fairness: Extreme client heterogeneity in IoT-FL, both in data and hardware, poses serious convergence and fairness challenges. Pfeiffer et al. [24] analyse system-level disparities and advocate for client-specific adaptation layers. Carlini et al. [30] further highlight how adversarial alignment in neural networks can propagate biases, underscoring the need for fairness constraints in model design. Multi-prototype FL, as discussed in the Wevolver report [12], enables clients to specialise on subsets of prototypes that better represent their local distributions. Deng et al. [64] propose a hierarchical knowledge transfer scheme that separates global, cluster, and local models, reducing the negative transfer from outlier clients. Formal fairness-aware FL protocols, however, are still lacking.

 doi:10.20944/preprints202504.2082.v1

Practical Privacy Guarantees: Applying PETs to LLM-based FL is non-trivial. While traditional DP mechanisms such as those in [38,41] remain foundational, Ahmadi et al. [42] show that when applied to LLMs in FL, DP introduces substantial performance degradation unless combined with hybrid masking and adaptive clipping strategies. Liu et al. [61] propose DP-LoRA, which selectively adds noise only to low-rank adaptation matrices, achieving a trade-off between utility and formal privacy. Yet, computational cost remains high. HE and SMPC offer stronger privacy but with significant communication and computational overheads unsuitable for IoT [46,48]. Efficient and scalable PET integration into low-power FL deployments remains an open issue.

Advanced Security and Trust: Foundation models open new attack surfaces in FL. Li et al. [109] demonstrate that compromised foundation models can inject imperceptible backdoors into global models during federated fine-tuning. Wu et al. [110] study adversarial adaptations where model updates mimic benign behaviour, bypassing current anomaly detection. Existing aggregation defenses like Krum [107] and Bulyan [117] struggle when attackers use model-aligned poisoning. Fan et al. [115] propose using zero-knowledge proofs for secure update verification in FL, though integration into LLM systems is yet to be tested. Decentralised trust frameworks with verifiable integrity, such as those discussed in [35], could mitigate these threats in IoT federations.

Standardisation and Benchmarking: Most existing FL benchmarks are designed for small NLP tasks (e.g., FedNLP [89]), lacking scale and modality diversity. Zhang et al. [88] introduce FederatedGPT to benchmark instruction tuning under FL settings, incorporating metrics like alignment score and robustness. FederatedScope-LLM [87] goes further, providing end-to-end support for parameter-efficient tuning (e.g., LoRA, prompt tuning) across diverse datasets. However, neither covers streaming sensor data, nor evaluates under network constraints typical in IoT. A comprehensive benchmark must include multimodal tasks, model size variability, privacy/utility/fairness trade-offs, and realistic simulation environments [120].

Multimodal Federated Learning: IoT deployments naturally involve multimodal data. ImageBind [121] demonstrates cross-modal LLMs trained on image, audio, depth, and IMU inputs in a single embedding space, but assumes centralised training. Cui et al. [96] highlight the challenges of decentralised multimodal alignment, including inter-client modality mismatch and unbalanced contributions. Communication-efficient multimodal fusion techniques and modality-specific adapters are needed. Sensor-based FL must incorporate asynchronous updates and cross-modal imputation to be practical in the wild.

Federated Learning for AI Agents: Li et al. [122] envision LLM-based AI agents capable of perception, planning, and actuation across decentralised IoT systems. Such agents require lifelong learning and task adaptation, which traditional FL lacks. PromptFL [71] proposes learning shared prompts instead of entire models, while FedPrompt [72] enhances this with privacy-preserving prompt updates. These methods significantly reduce communication and allow client-specific behaviour, but lack reasoning and memory modules required by generalist agents. Integration with reinforcement FL and safe exploration policies is a future direction.

Continual Learning and Adaptability: The temporal nature of IoT data leads to frequent concept drift. Shenaj et al. [123] propose online adaptation techniques but do not consider privacy. Wang et al. [98] review continual FL methods including regularisation-based and rehearsal-based strategies. Xia et al. [99] propose FCLLM-DT, which maintains temporal awareness via digital twins. These approaches should be enhanced with memory-efficient adaptation and forgettable modules that meet legal obligations on data deletion.

Legal, Ethical, and Economic Considerations: Federated LLMs operating across jurisdictions must comply with evolving data governance policies. Cheng et al. [10] outline open legal questions in multi-party FL, such as liability for biased decisions and model misuse. Qu et al. [13] emphasise ethical concerns such as disproportionate access to compute resources and biased training data. Lim et al. [36] review incentive mechanisms like token-based payments or fairness-based credit allocation,

 doi:10.20944/preprints202504.2082.v1

critical for encouraging client participation. However, these are rarely tested in LLM-specific scenarios, and no consensus exists on equitable reward strategies.

Machine Unlearning and Data Erasure: Hu et al. [124] propose erasing LoRA-tuned knowledge via gradient projection and local retraining to remove specific client data contributions without damaging generalisation. Patil et al. [125] leverage influence functions to reduce a sample's effect on final predictions, but require full access to model internals. Qiu et al. [126] address federated unlearning by designing reverse aggregation schemes, though practical validation on LLMs is absent. Verifiability and efficiency of unlearning remain open problems, especially in decentralised, heterogeneous FL contexts.

8. Conclusions

Bringing together the IoT , LLMs , and FL creates a powerful combination. This review has explored how this three-way synergy, backed by strong privacy techniques, paving the way for smarter, more responsive, and trustworthy distributed systems – achieving results that are not available when these technologies are used in pairs. We've mapped out the motivations, the edge-focused architectures, the key methods like PEFT and SFL that make it work, and importantly, the significant challenges involved. Making this powerful integration a reality means tackling some tough hurdles head-on. We need to find ways to run demanding LLMs on resource-limited IoT devices using FL, manage data sharing across networks without overwhelming them, handle the inherent diversity in IoT data and systems, and ensure fairness for everyone involved. Above all, protecting user privacy and securing the entire system against attack, all while meeting legal requirements, is absolutely critical. Despite these difficulties, researchers are actively finding solutions. We're seeing progress with techniques like model compression, smarter communication strategies, personalized learning, advanced privacy methods, and robust ways to combine model updates – though finding the right balance is always key. Encouragingly, real-world applications are starting to emerge, showing the clear value of using FL to let LLMs learn from distributed IoT data privately and effectively.

However, there's still a gap between this potential and widespread, reliable use. To close this gap, the research community needs to focus on several key areas. We urgently need breakthroughs in on-device efficiency for tiny edge devices, more robust algorithms that can handle messy real-world data and potential attacks, reliable ways to guarantee privacy and fairness, standard benchmarks to measure progress fairly, and clear thinking on the legal, ethical, and economic implications.By taking on these challenges with focused, collaborative research, we can unlock the true promise of this technological convergence. Getting this right means building a future with distributed AI systems that are not only powerful and efficient but also fundamentally trustworthy and respectful of data rights – impacting critical areas from industry to healthcare and beyond.

Author Contributions: Conceptualization and methodology, H.Y., X.Y., K.W., W.N.; software, H.Y.; validation, H.Y.; formal analysis, H.Y., X.Y.; investigation, H.Y., H.L.; resources, H.Y., H.L.; writing—original draft preparation, H.Y.; writing—review and editing, H.Y., H.L., X.Y., K.W., W.N., J.A.Z., R.P.L.; visualization, H.Y., X.Y., K.W., W.N.; supervision, X.Y., K.W., W.N.; project administration, J.A.Z., R.P.L.; funding acquisition, J.A.Z., R.P.L.. All authors have read and agreed to the published version of the manuscript.

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

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial Intelligence
CFL	Centralized Federated Learning
DFL	Decentralized Federated Learning
DP	Differential Privacy
FL	Federated Learning

 doi:10.20944/preprints202504.2082.v1

GDPR	General Data Protection Regulation
HE	Homomorphic Encryption
HIPAA	Health Insurance Portability and Accountability Act
IIoT	Industrial Internet of Things
IoT	Internet of Things
KD	Knowledge Distillation
LLM	Large Language Model
LoRA	Low-Rank Adaptation
Non-IID	Non-Independent and Identically Distributed
PEFT	Parameter-Efficient Fine-Tuning
PET	Privacy-Enhancing Technology
PFL	Personalized Federated Learning
PQC	Post-Quantum Cryptography
SFL	Split Federated Learning
SMPC	Secure Multi-Party Computation
TEE	Trusted Execution Environment
ZKP	Zero-Knowledge Proof

References

1. Brown, T.B.; Mann, B.; Ryder, N.; Subbiah, M.; Kaplan, J.D.; Dhariwal, P.; Neelakantan, A.; Shyam, P.; Sastry, G.; Askell, A.; et al. Language Models are Few-Shot Learners. In Proceedings of the Advances in Neural Information Processing Systems 33 (NeurIPS 2020); Larochelle, H.; Ranzato, M.; Hadsell, R.; Balcan, M.F.; Lin, H., Eds. Curran Associates, Inc., 2020, pp. 1877–1901.
2. Touvron, H.; Lavril, T.; Izacard, G.; Martinet, X.; Lachaux, M.A.; Lacroix, T.; Rozière, B.; Goyal, N.; Hambro, E.; Azhar, F.; et al. LLaMA: Open and Efficient Foundation Language Models. arXiv preprint arXiv:2302.13971, 2023, [arXiv:cs.CL/2302.13971].
3. Chen, X.; Wu, W.; Li, Z.; Li, L.; Ji, F. LLM-Empowered IoT for 6G Networks: Architecture, Challenges, and Solutions. *arXiv preprint arXiv:2503.13819* **2025**.
4. Kaplan, J.; McCandlish, S.; Henighan, T.; Brown, T.B.; Chess, B.; Child, R.; Gray, S.; Radford, A.; Wu, J.; Amodei, D. Scaling Laws for Neural Language Models. arXiv preprint arXiv:2001.08361, 2020, [arXiv:cs.LG/2001.08361].
5. Weidinger, L.; Mellor, J.; Rauh, M.; Griffin, C.; Uesato, J.; Huang, P.S.; Cheng, M.; Glaese, M.; Balle, B.; Kasirzadeh, A.; et al. Ethical and social risks of harm from Language Models. arXiv preprint arXiv:2112.04359, 2021, [arXiv:cs.CL/2112.04359].
6. Mao, Y.; You, C.; Zhang, J.; Huang, K.; Letaief, K.B. A survey on mobile edge computing: The communication perspective. *IEEE communications surveys & tutorials* **2017**, *19*, 2322–2358.
7. Wang, J.; Liu, Z.; Yang, X.; Li, M.; Lyu, Z. The Internet of Things under Federated Learning: A Review of the Latest Advances and Applications. *Computers, Materials and Continua* **2025**, *82*, 1–39.
8. Villalobos, P.; Sevilla, J.; Heim, L.; Besiroglu, T.; Hobbhahn, M.; Ho, A. Will We Run Out of Data? An Analysis of the Limits of Scaling Datasets in Machine Learning. arXiv preprint arXiv:2211.04325, 2022, [arXiv:cs.LG/2211.04325].
9. McMahan, B.; Moore, E.; Ramage, D.; Hampson, S.; y Arcas, B.A. Communication-efficient learning of deep networks from decentralized data. In Proceedings of the Artificial intelligence and statistics. PMLR, 2017, pp. 1273–1282.
10. Cheng, Y.; Zhang, W.; Zhang, Z.; Zhang, C.; Wang, S.; Mao, S. Towards Federated Large Language Models: Motivations, Methods, and Future Directions. *IEEE Communications Surveys & Tutorials* **2024**.
11. Li, K.; Yuan, X.; Zheng, J.; Ni, W.; Dressler, F.; Jamalipour, A. Leverage Variational Graph Representation for Model Poisoning on Federated Learning. *IEEE Transactions on Neural Networks and Learning Systems* **2025**, *36*, 116–128. https://doi.org/10.1109/TNNLS.2024.3394252.
12. Wevolver. Chapter 5: The Future of Edge AI. Available online: url:https://www.wevolver.com/article/2025-edge-ai-technology-report/the-future-of-edge-ai, 2025.
13. Qu, Y.; Ding, M.; Sun, N.; Thilakarathna, K.; Zhu, T.; Niyato, D. The frontier of data erasure: Machine unlearning for large language models, 2024.
14. Adam, M.; Baroud, U. Federated Learning For IoT: Applications, Trends, Taxonomy, Challenges, Current Solutions, and Future Directions. *IEEE Open Journal of the Communications Society* **2024**.

 doi:10.20944/preprints202504.2082.v1

15. Friha, O.; Ferrag, M.A.; Kantarci, B.; Cakmak, B.; Ozgun, A.; Ghoualmi-Zine, N. Llm-based edge intelligence: A comprehensive survey on architectures, applications, security and trustworthiness. *IEEE Open Journal of the Communications Society* **2024**.
16. Hu, E.J.; Shen, Y.; Wallis, P.; Allen-Zhu, Z.; Li, Y.; Wang, S.; Wang, L.; Chen, W. Lora: Low-rank adaptation of large language models. arXiv 2021. *arXiv preprint arXiv:2106.09685* **2021**.
17. Lin, Z.; Hu, X.; Zhang, Y.; Chen, Z.; Fang, Z.; Chen, X.; Li, A.; Vepakomma, P.; Gao, Y. Splitlora: A split parameter-efficient fine-tuning framework for large language models, 2024.
18. Wu, W.; Li, M.; Qu, K.; Zhou, C.; Shen, X.; Zhuang, W.; Li, X.; Shi, W. Split learning over wireless networks: Parallel design and resource management. *IEEE Journal on Selected Areas in Communications* **2023**, *41*, 1051–1066.
19. Chen, H.Y.; Tu, C.H.; Li, Z.; Shen, H.W.; Chao, W.L. On the importance and applicability of pre-training for federated learning. *arXiv preprint arXiv:2206.11488* **2022**.
20. Khan, L.U.; Saad, W.; Han, Z.; Hossain, E.; Hong, C.S. Federated learning for internet of things: Recent advances, taxonomy, and open challenges. *IEEE Communications Surveys & Tutorials* **2021**, *23*, 1759–1799.
21. Nguyen, D.C.; Ding, M.; Pathirana, P.N.; Seneviratne, A.; Li, J.; Poor, H.V. Federated learning for internet of things: A comprehensive survey. *IEEE Communications Surveys & Tutorials* **2021**, *23*, 1622–1658.
22. Liu, M.; Ho, S.; Wang, M.; Gao, L.; Jin, Y.; Zhang, H. Federated learning meets natural language processing: A survey. *arXiv preprint arXiv:2107.12603* **2021**.
23. Zhuang, W.; Chen, C.; Lyu, L. When foundation model meets federated learning: Motivations, challenges, and future directions. *arXiv preprint arXiv:2306.15546* **2023**.
24. Pfeiffer, K.; Rapp, M.; Khalili, R.; Henkel, J. Federated learning for computationally constrained heterogeneous devices: A survey. *ACM Computing Surveys* **2023**, *55*, 1–27.
25. Xu, M.; Du, H.; Niyato, D.; Kang, J.; Xiong, Z.; Mao, S.; Han, Z.; Jamalipour, A.; Kim, D.I.; Shen, X.; et al. Unleashing the power of edge-cloud generative AI in mobile networks: A survey of AIGC services. *IEEE Communications Surveys & Tutorials* **2024**, *26*, 1127–1170.
26. Gong, X. Delay-optimal distributed edge computing in wireless edge networks. In Proceedings of the IEEE INFOCOM 2020-IEEE conference on computer communications. IEEE, 2020, pp. 2629–2638.
27. Ashish, V. Attention is all you need. *Advances in neural information processing systems* **2017**, *30*, I.
28. Lee, J.; Toutanova, K. Pre-training of deep bidirectional transformers for language understanding. *arXiv preprint arXiv:1810.04805* **2018**, *3*.
29. Ouyang, L.; Wu, J.; Jiang, X.; Almeida, D.; Wainwright, C.L.; Mishkin, P.; Zhang, C.; Agarwal, S.; Slama, K.; Ray, A.; et al. Training Language Models to Follow Instructions with Human Feedback. In Proceedings of the Advances in Neural Information Processing Systems 35 (NeurIPS 2022); Koyejo, S.; Mohamed, S.; Agarwal, A.; Belgrave, D.; Cho, K.; Oh, A., Eds. Curran Associates, Inc., 2022, pp. 27730–27744.
30. Carlini, N.; Nasr, M.; Choquette-Choo, C.A.; Jagielski, M.; Gao, I.; Koh, P.W.W.; Ippolito, D.; Tramer, F.; Schmidt, L. Are aligned neural networks adversarially aligned?, 2023.
31. Wu, N.; Yuan, X.; Wang, S.; Hu, H.; Xue, M. Cardinality Counting in" Alcatraz": A Privacy-aware Federated Learning Approach. In Proceedings of the Proceedings of the ACM Web Conference 2024, 2024, pp. 3076–3084.
32. Hu, S.; Yuan, X.; Ni, W.; Wang, X.; Hossain, E.; Vincent Poor, H. OFDMA-F²L: Federated Learning With Flexible Aggregation Over an OFDMA Air Interface. *IEEE Transactions on Wireless Communications* **2024**, *23*, 6793–6807. https://doi.org/10.1109/TWC.2023.3334691.
33. Bhavsar, M.; Bekele, Y.; Roy, K.; Kelly, J.; Limbrick, D. FL-IDS: Federated learning-based intrusion detection system using edge devices for transportation IoT. *IEEE Access* **2024**.
34. Tian, Y.; Wang, J.; Wang, Y.; Zhao, C.; Yao, F.; Wang, X. Federated vehicular transformers and their federations: Privacy-preserving computing and cooperation for autonomous driving. *IEEE Transactions on Intelligent Vehicles* **2022**, *7*, 456–465.
35. Beltrán, E.T.M.; Pérez, M.Q.; Sánchez, P.M.S.; Bernal, S.L.; Bovet, G.; Pérez, M.G.; Pérez, G.M.; Celdrán, A.H. Decentralized federated learning: Fundamentals, state of the art, frameworks, trends, and challenges. *IEEE Communications Surveys & Tutorials* **2023**, *25*, 2983–3013.
36. Witt, L.; Heyer, M.; Toyoda, K.; Samek, W.; Li, D. Decentral and incentivized federated learning frameworks: A systematic literature review. *IEEE Internet of Things Journal* **2022**, *10*, 3642–3663.
37. Li, T.; Sahu, A.K.; Talwalkar, A.; Smith, V. Federated learning: Challenges, methods, and future directions. *IEEE signal processing magazine* **2020**, *37*, 50–60.

 doi:10.20944/preprints202504.2082.v1

38. Dwork, C.; McSherry, F.; Nissim, K.; Smith, A. Calibrating noise to sensitivity in private data analysis. In Proceedings of the Theory of Cryptography: Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006. Proceedings 3. Springer, 2006, pp. 265–284.
39. Shan, B.; Yuan, X.; Ni, W.; Wang, X.; Liu, R.P.; Dutkiewicz, E. Preserving the privacy of latent information for graph-structured data. *IEEE Transactions on Information Forensics and Security* **2023**, *18*, 5041–5055.
40. Ragab, M.; Ashary, E.B.; Alghamdi, B.M.; Aboalela, R.; Alsaadi, N.; Maghrabi, L.A.; Allehaibi, K.H. Advanced artificial intelligence with federated learning framework for privacy-preserving cyberthreat detection in IoT-assisted sustainable smart cities. *Scientific Reports* **2025**, *15*, 4470.
41. Abadi, M.; Chu, A.; Goodfellow, I.; McMahan, H.B.; Mironov, I.; Talwar, K.; Zhang, L. Deep learning with differential privacy. In Proceedings of the Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, 2016, pp. 308–318.
42. Ahmadi, K.; et al.. An Interactive Framework for Implementing Privacy-Preserving Federated Learning: Experiments on Large Language Models. ResearchGate preprint, 2025.
43. Basu, P.; Roy, T.S.; Naidu, R.; Muftuoglu, Z.; Singh, S.; Mireshghallah, F. Benchmarking differential privacy and federated learning for bert models. *arXiv preprint arXiv:2106.13973* **2021**.
44. Hu, S.; Yuan, X.; Ni, W.; Wang, X.; Hossain, E.; Vincent Poor, H. Differentially Private Wireless Federated Learning With Integrated Sensing and Communication. *IEEE Transactions on Wireless Communications* **2025**, pp. 1–1. https://doi.org/10.1109/TWC.2025.3555212.
45. Yuan, X.; Ni, W.; Ding, M.; Wei, K.; Li, J.; Poor, H.V. Amplitude-Varying Perturbation for Balancing Privacy and Utility in Federated Learning. *IEEE Transactions on Information Forensics and Security* **2023**, *18*, 1884–1897. https://doi.org/10.1109/TIFS.2023.3258255.
46. Paillier, P. Public-key cryptosystems based on composite degree residuosity classes. In Proceedings of the International conference on the theory and applications of cryptographic techniques. Springer, 1999, pp. 223–238.
47. Shamir, A. How to share a secret. *Communications of the ACM* **1979**, *22*, 612–613.
48. Yao, A.C. Protocols for secure computations. In Proceedings of the 23rd annual symposium on foundations of computer science (sfcs 1982). IEEE, 1982, pp. 160–164.
49. Bonawitz, K.; Ivanov, V.; Kreuter, B.; Marcedone, A.; McMahan, H.B.; Patel, S.; Ramage, D.; Segal, A.; Seth, K. Practical secure aggregation for privacy-preserving machine learning. In Proceedings of the proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017, pp. 1175–1191.
50. Che, T.; Liu, J.; Zhou, Y.; Ren, J.; Zhou, J.; Sheng, V.S.; Dai, H.; Dou, D. Federated learning of large language models with parameter-efficient prompt tuning and adaptive optimization. *arXiv preprint arXiv:2310.15080* **2023**.
51. Lyu, L.; Yu, H.; Ma, X.; Chen, C.; Sun, L.; Zhao, J.; Yang, Q.; Philip, S.Y. Privacy and robustness in federated learning: Attacks and defenses. *IEEE transactions on neural networks and learning systems* **2022**.
52. Xi, Z.; Chen, W.; Guo, X.; He, W.; Ding, Y.; Hong, B.; Zhang, M.; Wang, J.; Jin, S.; Zhou, E.; et al. The rise and potential of large language model based agents: A survey. *Science China Information Sciences* **2025**, *68*, 121101.
53. Malaviya, S.; Shukla, M.; Lodha, S. Reducing communication overhead in federated learning for pre-trained language models using parameter-efficient finetuning. In Proceedings of the Conference on Lifelong Learning Agents. PMLR, 2023, pp. 456–469.
54. Jiang, J.; Jiang, H.; Ma, Y.; Liu, X.; Fan, C. Low-parameter federated learning with large language models, 2024.
55. Gu, Y.; Dong, L.; Wei, F.; Huang, M. MiniLLM: Knowledge distillation of large language models. *arXiv preprint arXiv:2306.08543* **2023**.
56. Naik, K. LLM fine tuning with LoRA, 2025.
57. Dettmers, T.; Pagnoni, A.; Holtzman, A.; Zettlemoyer, L. Qlora: Efficient finetuning of quantized llms. *Advances in neural information processing systems* **2023**, *36*, 10088–10115.
58. Frantar, E.; Alistarh, D. SparseGPT: Massive Language Models Can Be Accurately Pruned in One-Shot. In Proceedings of the Proceedings of the 40th International Conference on Machine Learning (ICML); Krause, A.; Brunskill, E.; Cho, K.; Engelhardt, B.; Sabato, S.; Scarlett, J., Eds., Honolulu, HI, USA, July 2023; Vol. 202, *Proceedings of Machine Learning Research*, pp. 10280–10295.
59. Xiao, G.; Lin, J.; Seznec, M.; Wu, H.; Demouth, J.; Han, S. SmoothQuant: Accurate and Efficient Post-Training Quantization for Large Language Models. In Proceedings of the Proceedings of the 40th International Conference on Machine Learning (ICML); Krause, A.; Brunskill, E.; Cho, K.; Engelhardt, B.; Sabato, S.;

 doi:10.20944/preprints202504.2082.v1

Scarlett, J., Eds., Honolulu, HI, USA, July 2023; Vol. 202, *Proceedings of Machine Learning Research*, pp. 38087–38099.

60. Tian, Y.; Wan, Y.; Lyu, L.; Yao, D.; Jin, H.; Sun, L. FedBERT: When federated learning meets pre-training. *ACM Transactions on Intelligent Systems and Technology (TIST)* **2022**, *13*, 1–26.
61. Liu, X.Y.; Zhu, R.; Zha, D.; Gao, J.; Zhong, S.; White, M.; Qiu, M. Differentially private low-rank adaptation of large language model using federated learning, 2025.
62. Zhang, Z.; Yang, Y.; Dai, Y.; Wang, Q.; Yu, Y.; Qu, L.; Xu, Z. FedPETuning: When federated learning meets the parameter-efficient tuning methods of pre-trained language models. In Proceedings of the Annual Meeting of the Association of Computational Linguistics 2023. Association for Computational Linguistics (ACL), 2023, pp. 9963–9977.
63. Ghiasvand, S.; Alizadeh, M.; Pedarsani, R. Decentralized Low-Rank Fine-Tuning of Large Language Models, 2025.
64. Deng, Y.; Ren, J.; Tang, C.; Lyu, F.; Liu, Y.; Zhang, Y. A hierarchical knowledge transfer framework for heterogeneous federated learning. In Proceedings of the IEEE INFOCOM 2023-IEEE Conference on Computer Communications. IEEE, 2023, pp. 1–10.
65. Fallah, A.; Mokhtari, A.; Ozdaglar, A. Personalized Federated Learning with Theoretical Guarantees: A Model-Agnostic Meta-Learning Approach. In Proceedings of the Advances in Neural Information Processing Systems 33 (NeurIPS 2020); Larochelle, H.; Ranzato, M.; Hadsell, R.; Balcan, M.F.; Lin, H., Eds. Curran Associates, Inc., 2020, pp. 3557–3568.
66. Collins, L.; Wu, S.; Oh, S.; Sim, K.C. PROFIT: Benchmarking Personalization and Robustness Trade-off in Federated Prompt Tuning. arXiv preprint arXiv:2310.04627, 2023, [arXiv:cs.LG/2310.04627].
67. Yang, F.E.; Wang, C.Y.; Wang, Y.C.F. Efficient model personalization in federated learning via client-specific prompt generation. In Proceedings of the Proceedings of the IEEE/CVF International Conference on Computer Vision, 2023, pp. 19159–19168.
68. Yi, L.; Yu, H.; Wang, G.; Liu, X.; Li, X. pFedLoRA: model-heterogeneous personalized federated learning with LoRA tuning. *arXiv preprint arXiv:2310.13283* **2023**.
69. Cho, Y.J.; Liu, L.; Xu, Z.; Fahrezi, A.; Joshi, G. Heterogeneous lora for federated fine-tuning of on-device foundation models. *arXiv preprint arXiv:2401.06432* **2024**.
70. Su, S.; Li, B.; Xue, X. Fedra: A random allocation strategy for federated tuning to unleash the power of heterogeneous clients. In Proceedings of the European Conference on Computer Vision. Springer, 2024, pp. 342–358.
71. Guo, T.; Guo, S.; Wang, J.; Tang, X.; Xu, W. Promptfl: Let federated participants cooperatively learn prompts instead of models–federated learning in age of foundation model. *IEEE Transactions on Mobile Computing* **2023**, *23*, 5179–5194.
72. Zhao, H.; Du, W.; Li, F.; Li, P.; Liu, G. Fedprompt: Communication-efficient and privacy-preserving prompt tuning in federated learning. In Proceedings of the ICASSP 2023-2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2023, pp. 1–5.
73. Chen, Y.; Chen, Z.; Wu, P.; Yu, H. FedOBD: Opportunistic block dropout for efficiently training large-scale neural networks through federated learning. *arXiv preprint arXiv:2208.05174* **2022**.
74. Sun, G.; Mendieta, M.; Luo, J.; Wu, S.; Chen, C. Fedperfix: Towards partial model personalization of vision transformers in federated learning. In Proceedings of the Proceedings of the IEEE/CVF international conference on computer vision, 2023, pp. 4988–4998.
75. Chen, D.; Yao, L.; Gao, D.; Ding, B.; Li, Y. Efficient personalized federated learning via sparse model-adaptation. In Proceedings of the International conference on machine learning. PMLR, 2023, pp. 5234–5256.
76. Cho, Y.J.; Manoel, A.; Joshi, G.; Sim, R.; Dimitriadis, D. Heterogeneous ensemble knowledge transfer for training large models in federated learning. *arXiv preprint arXiv:2204.12703* **2022**.
77. Sui, D.; Chen, Y.; Zhao, J.; Jia, Y.; Xie, Y.; Sun, W. Feded: Federated learning via ensemble distillation for medical relation extraction. In Proceedings of the Proceedings of the 2020 conference on empirical methods in natural language processing (EMNLP), 2020, pp. 2118–2128.
78. Mei, H.; Cai, D.; Wu, Y.; Wang, S.; Xu, M. A Survey of Backpropagation-free Training For LLMS, 2024.
79. Xu, M.; Wu, Y.; Cai, D.; Li, X.; Wang, S. Federated Fine-tuning of Billion-sized Language Models Across Mobile Devices. arXiv preprint arXiv:2308.13894, 2023, [arXiv:cs.LG/2308.13894].
80. Qin, Z.; Chen, D.; Qian, B.; Ding, B.; Li, Y.; Deng, S. Federated full-parameter tuning of billion-sized language models with communication cost under 18 kilobytes. *arXiv preprint arXiv:2312.06353* **2023**.

 doi:10.20944/preprints202504.2082.v1

81. Sun, J.; Xu, Z.; Yin, H.; Yang, D.; Xu, D.; Chen, Y.; Roth, H.R. Fedbpt: Efficient federated black-box prompt tuning for large language models. *arXiv preprint arXiv:2310.01467* **2023**.
82. Pau, D.P.; Aymone, F.M. Suitability of forward-forward and pepita learning to mlcommons-tiny benchmarks. In Proceedings of the 2023 IEEE International Conference on Omni-layer Intelligent Systems (COINS). IEEE, 2023, pp. 1–6.
83. He, C.; Li, S.; So, J.; Zeng, X.; Zhang, M.; Wang, H.; Wang, X.; Vepakomma, P.; Singh, A.; Qiu, H.; et al. FedML: A Research Library and Benchmark for Federated Machine Learning. arXiv preprint arXiv:2007.13518, 2020, [arXiv:cs.LG/2007.13518].
84. Beutel, D.J.; Topal, T.; Mathur, A.; Qiu, X.; Fernandez-Marques, J.; Gao, Y.; Sani, L.; Li, K.H.; Parcollet, T.; de Gusmão, P.P.B.; et al. Flower: A Friendly Federated Learning Research Framework. arXiv preprint arXiv:2007.14390, 2020, [arXiv:cs.LG/2007.14390].
85. Arisdakessian, S.; Wahab, O.A.; Mourad, A.; Otrok, H.; Guizani, M. A survey on IoT intrusion detection: Federated learning, game theory, social psychology, and explainable AI as future directions, 2022.
86. Fan, T.; Kang, Y.; Ma, G.; Chen, W.; Wei, W.; Fan, L.; Yang, Q. FATE-LLM: A Industrial Grade Federated Learning Framework for Large Language Models. arXiv preprint arXiv:2310.10049, 2023, [arXiv:cs.LG/2310.10049].
87. Kuang, W.; Qian, B.; Li, Z.; Chen, D.; Gao, D.; Pan, X.; Xie, Y.; Li, Y.; Ding, B.; Zhou, J. Federatedscope-llm: A comprehensive package for fine-tuning large language models in federated learning. In Proceedings of the Proceedings of the 30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, 2024, pp. 5260–5271.
88. Zhang, J.; Vahidian, S.; Kuo, M.; Li, C.; Zhang, R.; Yu, T.; Wang, G.; Chen, Y. Towards Building The Federatedgpt: Federated Instruction Tuning. In Proceedings of the ICASSP, 2024.
89. Lin, B.Y.; He, C.; Zeng, Z.; Wang, H.; Huang, Y.; Dupuy, C.; Gupta, R.; Soltanolkotabi, M.; Ren, X.; Avestimehr, S. FedNLP: Benchmarking Federated Learning Methods for Natural Language Processing Tasks. arXiv preprint arXiv:2104.08815, 2021, [arXiv:cs.CL/2104.08815].
90. Ye, R.; Wang, W.; Chai, J.; Li, D.; Li, Z.; Xu, Y.; Du, Y.; Wang, Y.; Chen, S. Openfedllm: Training large language models on decentralized private data via federated learning. In Proceedings of the Proceedings of the 30th ACM SIGKDD conference on knowledge discovery and data mining, 2024, pp. 6137–6147.
91. Chakshu, N.K.; Nithiarasu, P. Orbital learning: a novel, actively orchestrated decentralised learning for healthcare. *Scientific Reports* **2024**, *14*, 10459.
92. Nguyen, J.; Malik, K.; Zhan, H.; Yousefpour, A.; Rabbat, M.; Malek, M.; Huba, D. Federated learning with buffered asynchronous aggregation. In Proceedings of the International conference on artificial intelligence and statistics. PMLR, 2022, pp. 3581–3607.
93. Charles, Z.; Mitchell, N.; Pillutla, K.; Reneer, M.; Garrett, Z. Towards federated foundation models: Scalable dataset pipelines for group-structured learning. *Advances in Neural Information Processing Systems* **2023**, *36*, 32299–32327.
94. Zhang, T.; Feng, T.; Alam, S.; Dimitriadis, D.; Lee, S.; Zhang, M.; Narayanan, S.S.; Avestimehr, S. Gpt-fl: Generative pre-trained model-assisted federated learning. *arXiv preprint arXiv:2306.02210* **2023**.
95. Wang, B.; Zhang, Y.J.; Cao, Y.; Li, B.; McMahan, H.B.; Oh, S.; Xu, Z.; Zaheer, M. Can public large language models help private cross-device federated learning? *arXiv preprint arXiv:2305.12132* **2023**.
96. Cui, C.; Ma, Y.; Cao, X.; Ye, W.; Zhou, Y.; Liang, K.; Chen, J.; Lu, J.; Yang, Z.; Liao, K.D.; et al. A Survey on Multimodal Large Language Models for Autonomous Driving. In Proceedings of the Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision (WACV), Waikoloa, HI, USA, January 2024; pp. 958–979.
97. Pandya, S.; Srivastava, G.; Jhaveri, R.; Babu, M.R.; Bhattacharya, S.; Maddikunta, P.K.R.; Mastorakis, S.; Piran, M.J.; Gadekallu, T.R. Federated learning for smart cities: A comprehensive survey. *Sustainable Energy Technologies and Assessments* **2023**, *55*, 102987.
98. Wang, L.; Zhang, X.; Su, H.; Zhu, J. A comprehensive survey of continual learning: Theory, method and application. *IEEE Transactions on Pattern Analysis and Machine Intelligence* **2024**.
99. Xia, Y.; Chen, Y.; Zhao, Y.; Kuang, L.; Liu, X.; Hu, J.; Liu, Z. FCLLM-DT: Enpowering Federated Continual Learning with Large Language Models for Digital Twin-based Industrial IoT. *IEEE Internet of Things Journal* **2024**.
100. Fang, M.; Cao, X.; Jia, J.; Gong, N.Z. Local Model Poisoning Attacks to Byzantine-Robust Federated Learning. In Proceedings of the Proceedings of the 29th USENIX Security Symposium (USENIX Security 20), Virtual Event, August 2020; pp. 1605–1622.

 doi:10.20944/preprints202504.2082.v1

101. Melis, L.; Song, C.; De Cristofaro, E.; Shmatikov, V. Exploiting unintended feature leakage in collaborative learning. In Proceedings of the 2019 IEEE symposium on security and privacy (SP). IEEE, 2019, pp. 691–706.
102. Yang, Y.; Dang, S.; Zhang, Z. An adaptive compression and communication framework for wireless federated learning. *IEEE Transactions on Mobile Computing* **2024**.
103. Hu, C.H.; Chen, Z.; Larsson, E.G. Scheduling and aggregation design for asynchronous federated learning over wireless networks. *IEEE Journal on Selected Areas in Communications* **2023**, *41*, 874–886.
104. Vahidian, S.; Morafah, M.; Chen, C.; Shah, M.; Lin, B. Rethinking data heterogeneity in federated learning: Introducing a new notion and standard benchmarks. *IEEE Transactions on Artificial Intelligence* **2023**, *5*, 1386–1397.
105. Zhu, L.; Liu, Z.; Han, S. Deep Leakage from Gradients. In Proceedings of the Advances in Neural Information Processing Systems 32 (NeurIPS 2019); Wallach, H.; Larochelle, H.; Beygelzimer, A.; d'Alché Buc, F.; Fox, E.; Garnett, R., Eds. Curran Associates, Inc., 2019, pp. 14774–14784.
106. Bagdasaryan, E.; Veit, A.; Hua, Y.; Estrin, D.; Shmatikov, V. How to Backdoor Federated Learning. In Proceedings of the Proceedings of the 23rd International Conference on Artificial Intelligence and Statistics (AISTATS); Chiappa, S.; Calandra, R., Eds., Palermo, Italy, August 2020; Vol. 108, *Proceedings of Machine Learning Research*, pp. 2938–2948.
107. Blanchard, P.; El Mhamdi, E.M.; Guerraoui, R.; Stainer, J. Machine Learning with Adversaries: Byzantine Tolerant Gradient Descent. In Proceedings of the Advances in Neural Information Processing Systems 30 (NIPS 2017); Guyon, I.; Luxburg, U.V.; Bengio, S.; Wallach, H.; Fergus, R.; Vishwanathan, S.; Garnett, R., Eds. Curran Associates, Inc., 2017, pp. 119–129.
108. Li, C.; Pang, R.; Xi, Z.; Du, T.; Ji, S.; Yao, Y.; Wang, T. An embarrassingly simple backdoor attack on self-supervised learning. In Proceedings of the Proceedings of the IEEE/CVF International Conference on Computer Vision, 2023, pp. 4367–4378.
109. Li, X.; Wang, S.; Wu, C.; Zhou, H.; Wang, J. Backdoor threats from compromised foundation models to federated learning. *arXiv preprint arXiv:2311.00144* **2023**.
110. Wu, C.; Li, X.; Wang, J. Vulnerabilities of foundation model integrated federated learning under adversarial threats, 2024.
111. Sun, H.; Zhang, Y.; Zhuang, H.; Li, J.; Xu, Z.; Wu, L. PEAR: privacy-preserving and effective aggregation for byzantine-robust federated learning in real-world scenarios. *The Computer Journal* **2025**, p. bxae086.
112. Gu, Z.; Yang, Y. Detecting malicious model updates from federated learning on conditional variational autoencoder. In Proceedings of the 2021 IEEE international parallel and distributed processing symposium (IPDPS). IEEE, 2021, pp. 671–680.
113. Zhang, Z.; Cao, X.; Jia, J.; Gong, N.Z. Fldetector: Defending federated learning against model poisoning attacks via detecting malicious clients. In Proceedings of the Proceedings of the 28th ACM SIGKDD conference on knowledge discovery and data mining, 2022, pp. 2545–2555.
114. Huang, W.; Wang, Y.; Cheng, A.; Zhou, A.; Yu, C.; Wang, L. A fast, performant, secure distributed training framework for LLM. In Proceedings of the ICASSP 2024-2024 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2024, pp. 4800–4804.
115. Fan, Y.; Zhu, R.; Wang, Z.; Wang, C.; Tang, H.; Dong, Y.; Cho, H.; Ohno-Machado, L. ByzSFL: Achieving Byzantine-Robust Secure Federated Learning with Zero-Knowledge Proofs, 2025.
116. 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. IEEE, 2021, pp. 1–10.
117. Guerraoui, R.; Rouault, S.; others. The Hidden Vulnerability of Distributed Learning in Byzantium. In Proceedings of the Proceedings of the 35th International Conference on Machine Learning (ICML); Dy, J.; Krause, A., Eds., Stockholm, Sweden, July 2018; Vol. 80, *Proceedings of Machine Learning Research*, pp. 1863–1872.
118. Li, S.; Ngai, E.C.H.; Voigt, T. An experimental study of byzantine-robust aggregation schemes in federated learning. *IEEE Transactions on Big Data* **2023**.
119. Wu, Z.; Ling, Q.; Chen, T.; Giannakis, G.B. Federated variance-reduced stochastic gradient descent with robustness to byzantine attacks. *IEEE Transactions on Signal Processing* **2020**, *68*, 4583–4596.
120. Zhou, T.; Yan, H.; Han, B.; Liu, L.; Zhang, J. Learning a robust foundation model against clean-label data poisoning attacks at downstream tasks. *Neural Networks* **2024**, *169*, 756–763.

 doi:10.20944/preprints202504.2082.v1

121. Girdhar, R.; El-Nouby, A.; Liu, Z.; Singh, M.; Alwala, K.V.; Joulin, A.; Misra, I. Imagebind: One embedding space to bind them all. In Proceedings of the Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, 2023, pp. 15180–15190.
122. Li, Y.; Wen, H.; Wang, W.; Li, X.; Yuan, Y.; Liu, G.; Liu, J.; Xu, W.; Wang, X.; Sun, Y.; et al. Personal llm agents: Insights and survey about the capability, efficiency and security. *arXiv preprint arXiv:2401.05459* **2024**.
123. Shenaj, D.; Toldo, M.; Rigon, A.; Zanuttigh, P. Asynchronous federated continual learning. In Proceedings of the Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2023, pp. 5055–5063.
124. Hu, Z.; Zhang, Y.; Xiao, M.; Wang, W.; Feng, F.; He, X. Exact and efficient unlearning for large language model-based recommendation, 2024.
125. Patil, V.; Hase, P.; Bansal, M. Can sensitive information be deleted from llms? objectives for defending against extraction attacks. *arXiv preprint arXiv:2309.17410* **2023**.
126. Qiu, X.; Shen, W.F.; Chen, Y.; Cancedda, N.; Stenetorp, P.; Lane, N.D. Pistol: Dataset compilation pipeline for structural unlearning of llms. *arXiv preprint arXiv:2406.16810* **2024**.