International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

Privacy-Aware AI in cloud-telecom convergence: A federated learning framework for secure data sharing

Adedeji Ojo Oladejo [1], Motunrayo Adebayo [2], David Olufemi [3,*], Eunice Kamau [4], Deligent Bobie-Ansah [5] and Daniel Williams [1]

[1] *School of Emerging Communication Technologies, Ohio University, Athens, Ohio, USA.*
[2] *Indiana Wesleyan University, Indiana, USA.*
[3] *Department of Computer Science & Engineering, University of Fairfax, USA.*
[4] *Depa Maharishi International University, Fairfield, Iowa, USA.*
[5] *Information and Telecommunication Systems, Ohio University, United States.*

International Journal of Science and Research Archive, 2025, 15(01), 005-022

Publication history: Received on 23 February 2025; revised on 28 March 2025; accepted on 31 March 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.15.1.0940

Abstract

With the increasing demand for integrated cloud and telecommunications (cloud-telecom convergence), the need for privacy-preserving artificial intelligence (AI) models has never been more urgent. Federated learning (FL) has emerged as a powerful framework that facilitates secure and privacy-aware machine learning models, without the need to share raw data between entities. This paper explores the role of federated learning in ensuring secure data sharing within cloud-telecom convergence, with a focus on privacy preservation. We discuss the fundamental concepts of privacy-aware AI, cloud-telecom integration, and federated learning. Moreover, we highlight the challenges, key research directions, and practical implementations of these technologies to achieve secure and scalable data sharing in 5G/6G environments. Through a systematic review of recent advances and future trends, we demonstrate the promise of federated learning in enabling privacy-preserving AI solutions in this domain.

Keywords: Privacy-aware AI; Cloud-Telecom Convergence; Federated Learning; Secure Data Sharing; 5G; Data Privacy; Artificial Intelligence; Telecommunications; Machine Learning; Privacy Preservation; Non-Identically Distributed; Cloud Computing

1. Introduction

The convergence of cloud computing and telecommunications (cloud-telecom convergence, CTC) represents a significant transformation in the way data is managed and services are delivered. As 5G and upcoming 6G technologies gain momentum, the convergence of cloud infrastructure with telecom networks allows for greater scalability, flexibility, and cost efficiency in providing advanced services such as edge computing, real-time data processing, and enhanced connectivity. This integration paves the way for innovative services that leverage the advantages of both cloud platforms and telecom networks, including global reach, low latency, and high bandwidth. However, the rapid growth in data generation, coupled with the need for ubiquitous connectivity, raises serious privacy concerns as sensitive user information is collected, stored, and processed in these environments.

Telecom operators handle vast amounts of sensitive data, including personal information such as call records, location data, and internet usage patterns. This large-scale data processing within a cloud-telecom infrastructure creates significant risks related to data breaches, unauthorized access, and non-compliance with data privacy regulations such as the General Data Protection Regulation (GDPR) in the EU and the California Consumer Privacy Act (CCPA) in the US.

* Corresponding author: David Olufemi

Thus, ensuring privacy and data protection is a critical concern in this context, particularly when deploying AI models to analyze and process sensitive information.

Artificial intelligence (AI) has become an integral part of the cloud-telecom convergence ecosystem. AI algorithms, particularly machine learning (ML) and deep learning (DL), are increasingly used to enhance services such as network optimization, traffic management, predictive maintenance, and customer behavior analysis. These AI models often require large datasets to train, which presents a dilemma: AI models need access to vast amounts of data to function effectively, but transmitting raw data from end devices to centralized data centers compromises privacy. This tension between the need for data and the need for privacy calls for innovative solutions that allow data to be processed securely without compromising confidentiality.

To address these privacy concerns, privacy-preserving AI techniques have been proposed, with one of the most promising approaches being Federated Learning (FL). Federated learning is a decentralized machine learning framework that enables the training of AI models across multiple devices (or edge nodes) without requiring data to be shared or transferred to a central server. Instead, only model updates, which represent the learned patterns from the data, are exchanged. This approach ensures that sensitive data remains on the local devices, preserving privacy while still benefiting from collaborative learning across a network. Federated learning has gained significant attention for its ability to balance privacy and utility in environments where data cannot be centralized due to privacy or regulatory concerns. Recent studies suggest that federated learning can be particularly advantageous in telecom networks, where data privacy is of utmost importance but the need for AI-driven insights is also critical.

Federated learning application within cloud-telecom convergence offers numerous benefits, including:

- **Data Privacy**: By design, FL allows data to remain local, significantly reducing the risk of unauthorized access and ensuring compliance with stringent data protection regulations (McMahan, Moore, & Ramage, 2017).
- **Efficiency and Scalability**: FL can efficiently handle large-scale deployments across millions of devices without burdening centralized systems with massive data loads (Kairouz, McMahan, & Suresh, 2019).
- **Reduced Latency**: By processing data closer to the edge of the network, federated learning can reduce the latency associated with cloud-based computation, leading to faster model training and inference (Zhang & Wang, 2020).

Despite its potential, federated learning in cloud-telecom convergence faces several challenges. These include data heterogeneity, where data from different devices may be inconsistent or non-iid (non-identically distributed), communication efficiency, where large-scale model updates can lead to high communication overhead, and security concerns, particularly the risk of model poisoning and other adversarial attacks that could undermine the trustworthiness of the model (Ghosh & Gupta, 2021). Additionally, the integration of federated learning into existing telecom infrastructure requires overcoming issues related to regulatory compliance, infrastructure compatibility, and resource constraints at the edge.

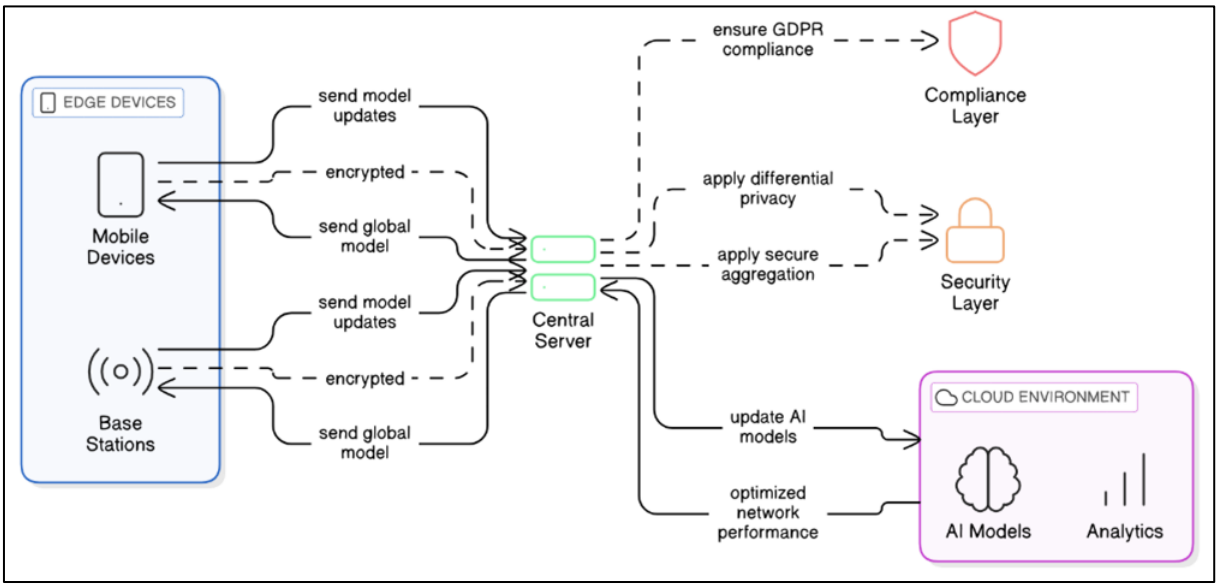

Figure 1 Privacy-Aware AI in Cloud-Telecom Convergence

This paper aims to explore the integration of federated learning within the context of privacy-preserving AI in cloud-telecom convergence. We delve into the fundamental concepts of federated learning, its benefits, and its challenges in this application. The goal is to identify how federated learning can be utilized to create secure, privacy-preserving frameworks for data sharing in telecom networks and to examine its potential for improving data privacy in the age of 5G and 6G. Furthermore, we provide an overview of current research trends and advancements in this field, highlighting key innovations and emerging solutions for overcoming the challenges associated with deploying federated learning in telecom environments.

In the following sections, we will discuss the architecture and principles of federated learning, explore its application within the telecom industry, and identify key research directions for the future. By understanding these critical elements, this paper seeks to contribute to the ongoing discussions on privacy-aware AI and secure data sharing within the ever-evolving landscape of cloud-telecom convergence.

2. Privacy-Aware AI in Cloud-Telecom Convergence

As cloud computing and telecommunications continue to converge, privacy becomes an increasingly important concern in ensuring that both users' personal data and organizational data remain protected. Telecom networks are built on vast infrastructures that generate, store, and transmit massive amounts of data. When combined with cloud platforms that aggregate this data for further analysis, the risks of data leakage, breaches, and unauthorized access rise significantly. In this context, privacy-aware AI techniques have become essential in allowing secure data sharing while maintaining the privacy of individuals and organizations. This chapter explores the various privacy-preserving techniques used in AI and how they are being integrated into cloud-telecom convergence environments.

2.1. Privacy-Preserving Techniques in AI

Privacy-preserving AI encompasses a broad range of technologies and techniques designed to ensure that data is kept confidential and protected from unauthorized access during machine learning and AI model development. These techniques aim to mitigate risks related to the exposure of sensitive data, such as personal identifiers, behavioral patterns, and financial information. Some of the most common privacy-preserving techniques include:

2.1.1. Differential Privacy (DP)

Differential Privacy (DP) is a powerful technique for ensuring that an individual’s data cannot be re-identified in a dataset, even if multiple datasets are combined or if an adversary has access to auxiliary information. The core principle of DP is that the output of a computation should not significantly change when an individual's data is added or removed from the dataset (Dwork, 2006). This ensures that the inclusion of any single data point does not impact on the overall results in a detectable manner.

In cloud-telecom convergence, DP can be applied to AI models where sensitive user data (e.g., call records, internet usage patterns) is anonymized, allowing AI models to be trained on statistical representations rather than raw data (Li et al., 2020). This method is particularly useful when sensitive data is shared between telecom providers and cloud platforms, ensuring that individual data privacy is maintained while still enabling valuable insights to be extracted.

2.1.2. Homomorphic Encryption (HE)

Homomorphic encryption (HE) allows computations to be performed on encrypted data, without the need to decrypt it. The results of these computations are also encrypted, ensuring that sensitive information remains private throughout the process. This is particularly valuable in cloud environments where sensitive user data may need to be processed by cloud service providers without exposing the raw data to them (Gentry, 2009).

In the context of cloud-telecom convergence, HE can enable privacy-preserving machine learning by allowing telecom providers to encrypt user data before sending it to a cloud-based AI model for analysis, while still allowing the model to perform computations such as classification or regression on the encrypted data. The encrypted results are then decrypted by the authorized user or telecom provider without exposing the underlying sensitive information.

2.1.3. Secure Multi-Party Computation (SMPC)

Secure Multi-Party Computation (SMPC) is a cryptographic technique that enables multiple parties to jointly compute a function over their private inputs while keeping those inputs confidential. The results of the computation can be shared, but no individual party learns anything about the others' private inputs (Goldwasser et al., 1989).

SMPC is highly applicable in cloud-telecom convergence, especially in multi-party scenarios such as collaborations between telecom operators, cloud providers, and third-party vendors. It allows for collaborative machine learning, where each party contributes to model training without revealing their individual data. For instance, telecom providers could use SMPC to jointly train a predictive model using their respective customer data, without disclosing sensitive details to one another (Zhu et al., 2020).

2.2. Challenges in Implementing Privacy-Aware AI in Cloud-Telecom Convergence

While privacy-preserving AI techniques such as differential privacy, homomorphic encryption, and secure multi-party computation offer powerful solutions, their implementation in cloud-telecom convergence is not without challenges. These challenges stem from the inherent nature of cloud and telecom networks, which often involve highly distributed data and computational resources.

2.2.1. Data Heterogeneity

One of the major challenges in privacy-aware AI within cloud-telecom convergence is the heterogeneity of data generated by different telecom nodes, users, and edge devices. Data from different devices often varies in format, quality, and type, which can complicate the development of uniform AI models. This challenge is particularly significant in the context of federated learning, where diverse data from mobile devices, base stations, and edge nodes need to be aggregated for training a global model. The non-iid (non-identically distributed) nature of this data can cause the model to perform poorly and reduce its ability to generalize across all devices (Li et al., 2018).

2.2.2. Communication Efficiency

Another challenge in cloud-telecom convergence is the communication efficiency required for privacy-aware AI techniques. In federated learning, for instance, model updates are communicated between edge devices and a central server. The volume of data exchanged between devices and the server can be substantial, especially in large-scale telecom environments. High communication overheads may lead to latency, network congestion, and increased costs. Optimizing this communication process while maintaining privacy is critical in large-scale implementations (Zhu et al., 2020).

2.2.3. Security Threats

Although privacy-preserving techniques protect individual data from unauthorized access, they are not immune to security threats. Adversaries can exploit weaknesses in cryptographic protocols or attack the model itself through methods such as model poisoning or data poisoning. In these types of attacks, malicious participants may send adversarial model updates or corrupt data to degrade the performance of the global AI model (Bhagoji et al., 2019). In the context of telecom networks, these vulnerabilities can lead to the compromise of the entire federated learning system, which may have severe consequences for service reliability and security.

2.2.4. Regulatory Compliance

In cloud-telecom convergence, ensuring compliance with privacy regulations is another significant challenge. Various countries and regions have enacted data protection laws, such as GDPR in Europe and CCPA in California, which impose strict regulations on how user data can be collected, stored, and processed. Federated learning and other privacy-aware AI techniques must adhere to these laws and integrating these techniques into existing telecom networks while ensuring full compliance is complex. The legal complexities around cross-border data sharing also add another layer of challenge (Zhang & Wang, 2020).

2.3. Future Directions

To address the challenges and harness the full potential of privacy-aware AI in cloud-telecom convergence, several future directions and innovations are necessary:

- **Edge Computing Integration**: The combination of federated learning with edge computing can reduce latency and improve the efficiency of AI training by processing data closer to where it is generated. This reduces communication overhead and improves response times, particularly in latency-sensitive applications like real-time network optimization (Zhang et al., 2021).
- **Blockchain for Secure Aggregation**: Blockchain technology can provide a secure, decentralized method for aggregating model updates in federated learning. It ensures that all updates are verifiable and tamper-proof, protecting the integrity of the AI model and mitigating the risks of model poisoning (Liang et al., 2019).

- **Adaptive Privacy-Preserving Techniques**: Future research could focus on developing adaptive privacy-preserving methods that can automatically adjust based on the privacy requirements of different data types. For example, more stringent privacy measures may be necessary for highly sensitive data, while less stringent methods could be applied to less sensitive information.

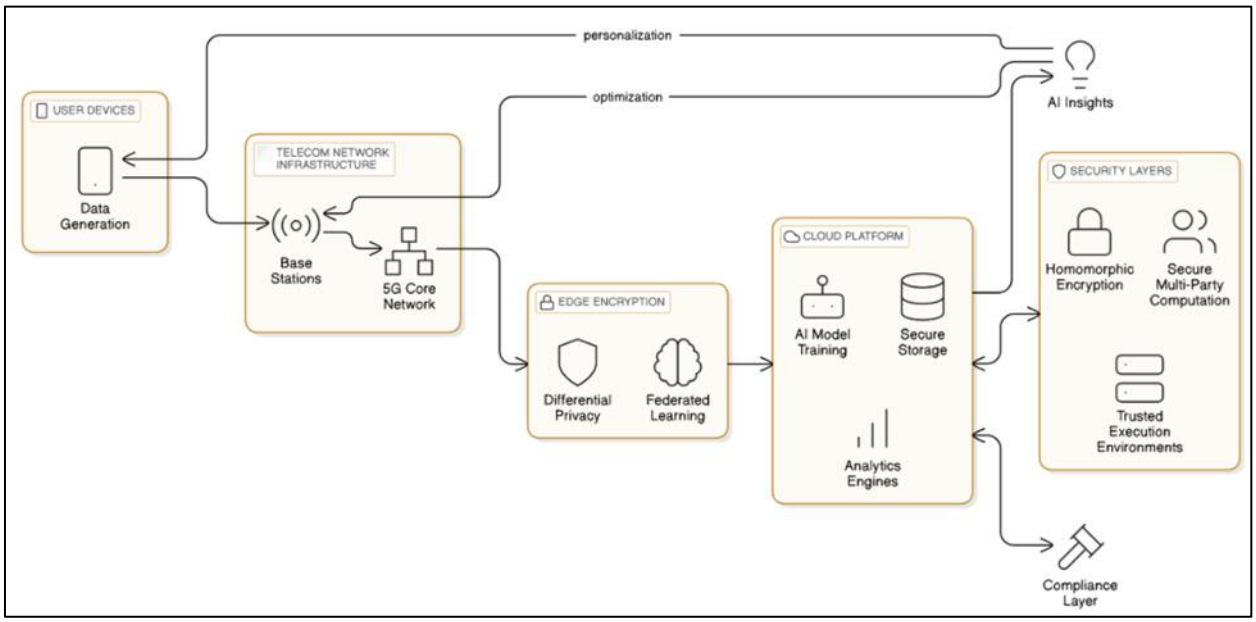

Figure 2 Privacy-Preserving AI Framework in Cloud-Telecom Convergence

Table 1 Comparison of Privacy-Preserving Techniques

Technique	Strengths	Limitations
Differential Privacy	Preserves privacy by adding noise	May reduce model accuracy
Homomorphic Encryption	Computations on encrypted data	High computational overhead
SMPC	Collaborative privacy-preserving learning	Complex setup and coordination

3. Federated Learning – A Privacy-Aware AI Framework

Federated learning (FL) has emerged as a transformative paradigm for privacy-preserving machine learning in distributed environments. Unlike traditional machine learning methods, which require centralized data collection, FL allows AI models to be trained collaboratively across multiple devices or institutions without ever sharing raw data. This approach is especially relevant in cloud-telecom convergence, where privacy, latency, and bandwidth efficiency are critical. By enabling decentralized model training, FL ensures compliance with privacy regulations while supporting scalable and efficient data-driven AI.

3.1. Foundations of Federated Learning

The core idea behind federated learning is to allow multiple parties—such as edge devices, base stations, or telecom operators—to train a shared model collaboratively while keeping their data local. Instead of sending raw data to a centralized server, each client trains the model on its local dataset and sends model gradients or parameter updates to the server, which aggregates them to improve the global model (McMahan et al., 2017).

$$w_{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} \boldsymbol{w_k}$$

w_{t+1} is the global model at iteration t+1,
n_k is the number of data samples on device k,
$\sum_{k=1}^{K} \frac{n_k}{n}$ is the total number of data samples,
$\boldsymbol{w_k}$ is the model update from device k.

This approach reduces data transfer costs and mitigates risks of data exposure, aligning with the data governance requirements of the telecom sector (Kairouz et al., 2021).

3.2. Types of Federated Learning

Federated learning can be categorized based on data distribution and organizational structure:

3.2.1. Horizontal Federated Learning (HFL)

HFL is used when participants share the same feature space but differs in their data samples. This is typical in telecom where several base stations might collect similar types of data (e.g., signal strength, user location) across different users. This model is ideal for training location-based traffic prediction systems without pooling user data centrally (Yang et al., 2019).

3.2.2. Vertical Federated Learning (VFL)

VFL applies when participants share the same users but differ in feature sets. For instance, a telecom operator and a bank may both serve the same customer base but hold different attributes about them. VFL allows these organizations to jointly train fraud detection models while preserving customer privacy (Hardy et al., 2017).

3.2.3. Federated Transfer Learning (FTL)

FTL is used when participants differ in both sample space and feature space. This is suitable when telecom operators collaborate with hospitals or retail companies to build models with limited overlapping data. FTL leverages pre-trained models and transfer learning to bridge domain gaps while protecting privacy (Liu et al., 2020).

3.3. Architecture of Federated Learning in Telecom Networks

A typical federated learning architecture in a telecom environment includes edge devices (UEs), local aggregators (e.g., base stations or MEC nodes), and a central cloud aggregator.

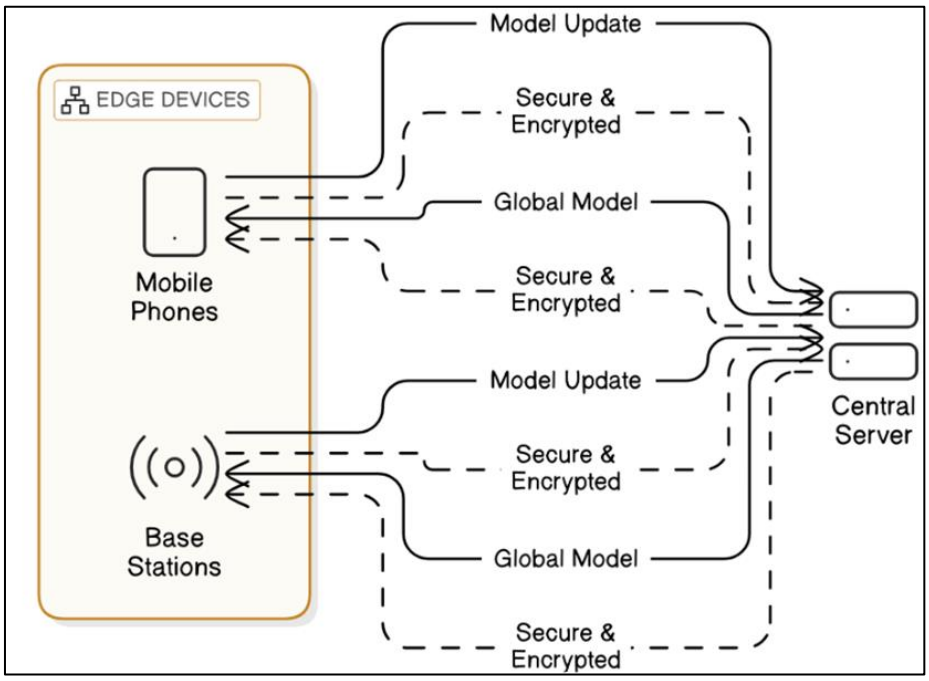

Figure 3 Federated Learning Architecture for Telecom Networks

This multi-tiered architecture aligns with 5G and 6G standards, where edge nodes possess sufficient compute capability to support AI training (Zhang et al., 2021). Local training reduces core network traffic and improves latency, while the centralized aggregator coordinates global model refinement.

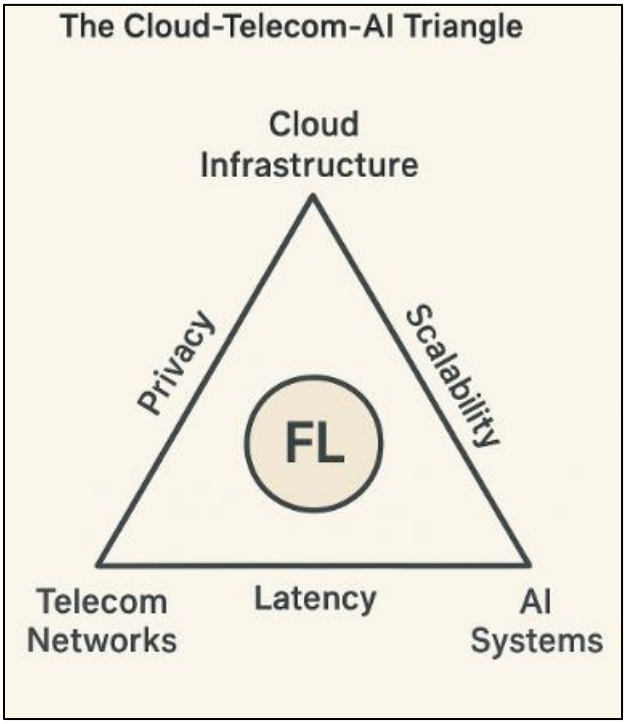

Figure 4 The Cloud-Telecom-AI Triangle

Above triangular diagram could be used to illustrate the synergy—and tension—between Cloud Infrastructure, AI Systems, and Telecom Networks, with Privacy, Latency, and Scalability at the three edges. FL sits at the center, mitigating conflicts among the three.

3.4. Key Advantages in Cloud-Telecom Convergence

Federated learning presents several distinct advantages in cloud-telecom integration:

3.4.1. Enhanced Privacy Compliance

As privacy regulations tighten worldwide, telecom operators must ensure that user data is never exposed to unauthorized entities. FL ensures data remains on-device, aligning with GDPR and CCPA mandates (Li et al., 2020).

3.4.2. Bandwidth and Latency Optimization

By processing data at the edge, FL significantly reduces the need to transmit large datasets across the network. Only lightweight model updates are exchanged, thus conserving bandwidth and improving real-time decision-making—critical in applications like handover optimization and traffic prediction (Shi et al., 2021).

3.4.3. Scalability and Heterogeneity Handling

FL can scale across millions of edge devices, accommodating diverse data distributions. Modern algorithms like FedAvg and FedProx can adapt to non-iid data, making federated learning viable even with heterogeneous data environments common in telecom systems (Li et al., 2020).

3.5. Use Cases in Telecommunications

3.5.1. Network Traffic Prediction

FL can be used to predict network congestion and optimize resource allocation by leveraging data from multiple base stations without centralizing the traffic logs. Local training ensures regional patterns are captured while preserving privacy (Zhao et al., 2020).

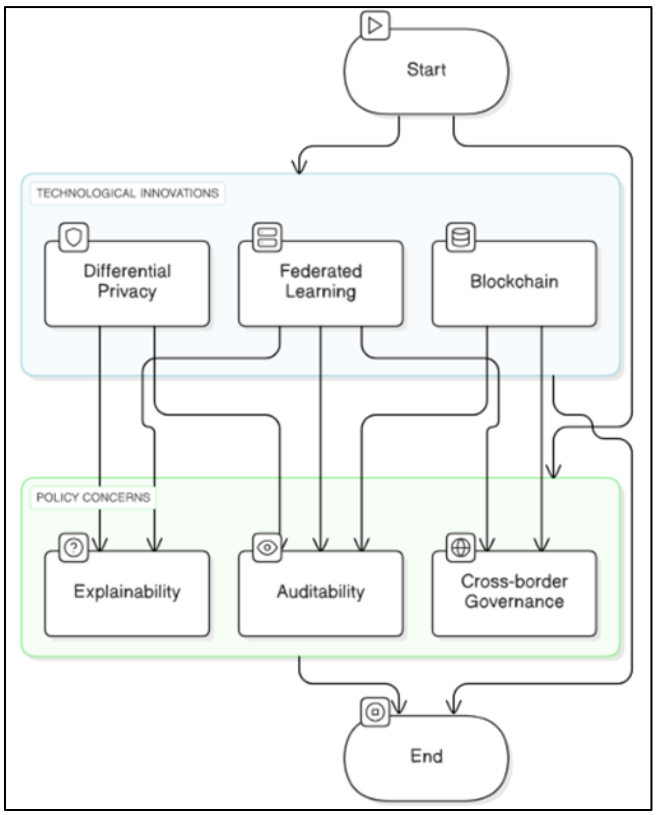

Figure 5 Policy-Technology Matrix

A 2D matrix could be shown aligning technological innovation (FL, blockchain, DP) with evolving policy concerns (auditability, cross-border governance, explainability).

3.5.2. User Behavior Analytics

Personalized models for churn prediction or service recommendations can be built using FL. Telecom operators can deploy models that learn from user behavior while ensuring the personal data never leaves the device (Bonawitz et al., 2019).

3.5.3. Fraud Detection and Anomaly Detection

FL allows collaborative model building across telecom firms or departments to detect fraudulent activities (e.g., SIM box fraud, account takeovers) without sharing raw transactional data (Liu et al., 2020).

3.5.4. Smart City and IoT Integration

In smart city deployments, telecom networks support thousands of sensors and devices. FL enables these devices to collaboratively train predictive maintenance or traffic control models without uploading raw sensor data to the cloud (Savazzi et al., 2020).

Table 2 Use Case Mapping of Federated Learning in Telecom

Use Case	FL Type	Privacy Benefit	Impact Area
Traffic Prediction	Horizontal FL	Local training of usage patterns	Network optimization
Fraud Detection (Cross-Sector)	Vertical FL	Shared learning without data exchange	Financial compliance
Personalized Services	Horizontal FL	On-device behavior analytics	Customer retention
Smart IoT Device Management	Federated TL	Transfer knowledge across device types	Smart infrastructure

4. Challenges in Implementing Federated Learning in Cloud-Telecom Convergence (Expanded)

Federated learning (FL) presents an innovative path to achieving privacy-aware AI in cloud-telecom convergence. However, its real-world deployment at scale—especially in the complex, data-intensive telecom landscape—is fraught with considerable challenges. These arise not only from the distributed nature of data and computation but also from the diversity of edge devices, the critical need for secure communication, and the requirements for compliance with privacy regulations. This chapter expands on the previously identified challenges by integrating further technical insights, deeper implications, and emerging strategies being explored in recent literature.

4.1. Data-Level Challenges (Extended)

4.1.1. Statistical Heterogeneity and Non-IID Data

Data heterogeneity, where devices generate statistically different data (non-IID), is the most cited challenge in federated learning literature. In telecom networks, different base stations or user equipment may observe varied data distributions due to user demographics, geographic location, and device types. As a result, the global model may underperform or diverge during aggregation (Li et al., 2020; Zhao et al., 2018).

This problem is exacerbated in cross-device FL, where the data on each node might contain only a small fraction of the entire input space. For example, users in a specific region may never encounter certain network conditions or application scenarios, resulting in local models with biased gradients (McMahan et al., 2017).

Recent research explores clustered FL and meta-learning techniques to build personalized yet generalizable models that respect local distributions while contributing to a shared global structure (Fallah et al., 2020; Sattler et al., 2020).

4.1.2. Data Imbalance and Temporal Drift

In telecom networks, data imbalance is frequent—certain types of events (e.g., dropped calls, network congestion) occur rarely compared to normal operation logs. This imbalance can skew the model to ignore critical but sparse classes (Sun et al., 2019). Moreover, user behaviors and network patterns evolve over time (known as concept drift), rendering previously learned models less effective.

To address these, continual learning frameworks and time-aware aggregation strategies are under investigation, which allow models to adapt incrementally to changing data distributions without catastrophic forgetting (Chen & Liu, 2018).

4.2. System-Level Challenges (Extended)

4.2.1. Communication Bottlenecks and Model Synchronization

Even though FL reduces the need to transfer raw data, it introduces heavy traffic in the form of iterative model updates. In telecom-grade networks involving thousands of nodes, such communication can overwhelm backhaul networks or edge routers. A single round of FL training with deep models (e.g., CNNs or LSTMs) may involve transmitting tens of megabytes per device, leading to delays and inefficiencies (Kairouz et al., 2021).

Update compression (e.g., sparse gradients, quantized models) and communication-efficient protocols like Federated Dropout (Caldas et al., 2019) are being proposed to mitigate this. These methods reduce the volume of transmitted data without degrading model quality.

4.2.2. Edge Device Constraints and Participation Volatility

Federated learning often relies on resource-constrained edge devices like mobile phones, IoT sensors, or small base stations. These devices may experience battery limitations, variable CPU/GPU availability, or unstable connectivity, leading to participation volatility.

Participation volatility can slow down training and introduce biases if only certain “reliable” devices consistently contribute updates. Strategies like device selection based on resource availability and asynchronous federated learning allow partial or delayed contributions while maintaining model convergence (Nishio & Yonetani, 2019).

Additionally, the "cold start problem" arises when newly onboarded nodes (e.g., new IoT deployments) have no prior participation history, requiring bootstrapping techniques using transferred models or synthetic data (Yurochkin et al., 2019).

4.3. Security and Privacy Challenges (Extended)

4.3.1. Malicious Client Behavior and Byzantine Attacks

FL's openness to untrusted participants increases the attack surface for Byzantine failures, where some clients act maliciously or provide corrupted updates to poison the global model. In a telecom scenario, such actions could compromise network prediction models, misguide resource allocation, or create security loopholes (Bagdasaryan et al., 2020).

Defensive aggregation mechanisms like Krum, Bulyan, or Median-based filtering are designed to exclude outlier updates and tolerate a bounded number of adversaries (Blanchard et al., 2017). These are being tailored to telecom-grade FL where large-scale deployments demand scalable yet robust defenses.

4.3.2. Gradient Leakage and Membership Inference

Even without direct data sharing, gradient-based inference attacks can reconstruct sensitive inputs from the model updates themselves. Studies have shown that image data, voice patterns, and even location traces can be partially reconstructed from gradient differences (Zhu et al., 2019). In telecom, this could lead to exposure of user call records or movement patterns.

Implementing differential privacy (DP) during model update sharing helps reduce such risks. However, DP introduces noise into the learning process, which may degrade model accuracy if not properly tuned. A trade-off emerges between privacy guarantees and utility (Abadi et al., 2016).

4.3.3. Secure Aggregation and Trust Models

To ensure that no party—including the server—can view individual client updates, Secure Aggregation protocols are employed. These cryptographic frameworks enable servers to compute aggregated updates without decrypting individual submissions (Bonawitz et al., 2017).

Emerging directions include federated trusted execution environments (TEEs) and blockchain-backed FL for auditability and transparency in FL workflows, especially relevant in multi-stakeholder telecom partnerships (Lu et al., 2020).

4.4. Legal, Ethical, and Operational Constraints

4.4.1. Regulatory Constraints and Cross-Border Data Sovereignty

Cloud-telecom convergence frequently spans regions with distinct **data residency laws**, such as the European GDPR, India's Data Protection Bill, and China's Personal Information Protection Law (PIPL). Even though FL retains data locally, questions remain about model ownership, data contribution tracing, and liability in case of model bias (Zhang & Wang, 2020).

Telecom operators must navigate these regulations while collaborating with cloud vendors and third-party service providers, requiring transparent logging, auditable FL systems, and model interpretability tools for legal compliance and accountability.

4.4.2. Deployment Costs and Ecosystem Complexity

Operationalizing federated learning in telecom infrastructures involves:

- Reengineering network topologies to support edge computation,
- Deploying containerized FL agents (e.g., using Docker or Kubernetes) on edge nodes,
- Monitoring model performance, security, and training fairness in a federated context.
- The **Total Cost of Ownership (TCO)** increases with the scale of deployment, especially when telecom providers must maintain heterogenous fleets of devices with secure communication, monitoring, and orchestration systems (Savazzi et al., 2020).

4.5. Research Directions for Overcoming Challenges

To address these challenges, researchers are focusing on:

- Adaptive FL frameworks that adjust learning rates, privacy budgets, and participation thresholds dynamically based on network conditions.
- Explainable FL, which seeks to make federated models interpretable to operators and regulators using tools like SHAP or LIME.
- Federated Reinforcement Learning (FRL) for dynamic telecom environments where policies evolve based on real-time feedback (Zhang et al., 2021).

4.6. Summary of Challenges and Solutions

In summary, while federated learning provides an appealing framework for privacy-aware AI in the age of cloud-telecom convergence, it is fraught with technical, legal, and infrastructural challenges. From managing statistical heterogeneity and communication overhead to ensuring security and regulatory compliance, the path to widespread deployment is complex and demands coordinated advances across multiple disciplines. Emerging research continues to explore solutions to these challenges, but real-world adoption will depend on how effectively these solutions can be operationalized at scale.

Table 3 Summary of Challenges and Mitigation Strategies

Challenge	Category	Mitigation
Non-IID Data	Data-Level	FedProx, personalized FL
Communication Overhead	System-Level	Compression, selective participation
Device Dropout	System-Level	Asynchronous FL, client sampling
Model Poisoning	Security	Robust aggregation, anomaly detection
Gradient Leakage	Privacy	Differential privacy, secure aggregation
Regulatory Compliance	Legal	Jurisdiction-aware deployment, audit logging
Operational Overhead	Operational	Edge orchestration frameworks

5. Practical Applications and Future Directions

Federated Learning (FL) in cloud-telecom convergence is not merely a conceptual solution to data privacy and security—it is increasingly being recognized as a practical enabler of real-world telecom services in the era of 5G, 6G, and massive Internet-of-Things (IoT) deployments. This chapter explores the evolving application areas of FL within the telecom landscape, from network optimization and anomaly detection to smart city services and user behavior modeling. In parallel, we also examine ongoing research and future directions, where federated learning is expected to become even more integrated, adaptive, and intelligent.

5.1. Network Traffic Forecasting and Optimization

One of the most prominent applications of federated learning in telecom environments is predictive network management. Modern telecom infrastructure must adapt in real-time to fluctuating network loads, varying user demand, and dynamic radio conditions. Historically, such adaptations required centralized data collection for model training, which raised concerns regarding user privacy and data sovereignty. Federated learning, however, allows edge

devices such as base stations and access points to locally train predictive models using real-time traffic data, which is then aggregated centrally to build a robust global model.

For instance, each base station can forecast its own traffic demand over time using local patterns, contributing only model updates to a central orchestration layer. This allows the telecom operator to preemptively allocate bandwidth, balance loads, and adjust routing strategies without direct access to granular traffic records (Zhang & Wang, 2020). The privacy-preserving nature of this model is especially important in enterprise and government use cases, where network data may be considered confidential.

A graphical representation here could depict a time-series comparison of predicted vs actual network usage, showing the improvement in prediction accuracy before and after applying FL-based traffic forecasting. Another graph could visualize the reduction in latency or packet loss due to FL-enabled dynamic resource allocation.

5.2. Anomaly Detection and Telecom Fraud Prevention

Anomaly detection remains a critical function in telecom operations, enabling the detection of SIM-box fraud, spamming, network intrusions, and malicious traffic. Traditional fraud detection systems rely on centralized data lakes that aggregate logs across multiple regions, increasing the risk of breaches and regulatory violations. With federated learning, each regional node or telecom gateway can analyze its traffic, detect patterns of normalcy, and collaboratively build a model that identifies deviations without exposing raw datasets (Liu et al., 2020).

This method is particularly effective for cross-border fraud detection, where telecom operators in different jurisdictions are hesitant—or legally prohibited—from sharing customer data. FL enables these operators to participate in joint fraud detection efforts while maintaining data privacy and sovereignty. The trained model becomes a global fraud detector, benefiting from the collective learning across telecom environments.

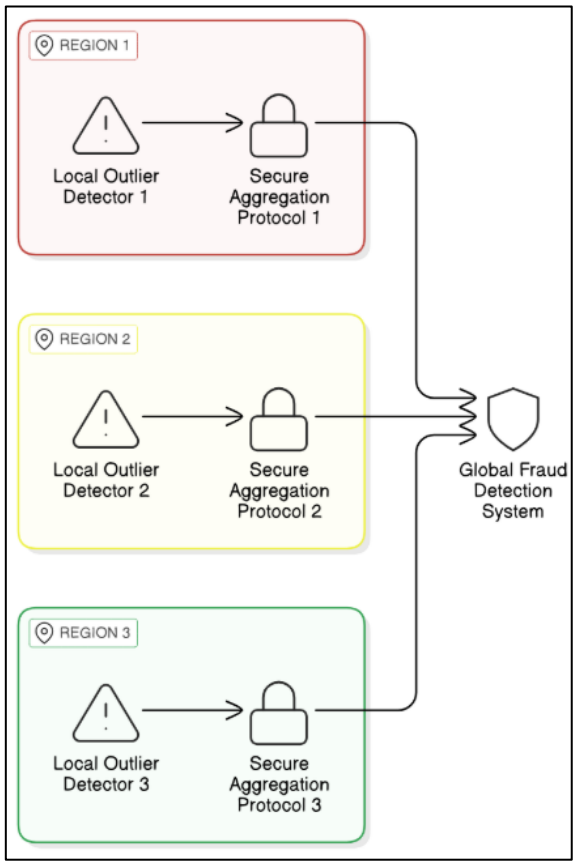

Figure 6 Heat map of detected anomalies across regions

5.3. Personalized Services and Churn Prediction

Telecom providers are increasingly investing in personalized customer experiences, such as tailored pricing plans, content recommendations, and proactive support. However, personalization inherently involves profiling user behavior, preferences, and communication habits—data that is sensitive and highly regulated.

Federated learning offers a solution where user personalization can happen locally, on-device or at the edge, while still benefiting from a shared learning process. For example, mobile devices can train models on individual usage patterns—app usage, browsing history, or call frequency—and contribute updates that help refine broader models for churn prediction or product targeting. Importantly, this entire process occurs without transmitting any individual's private usage data to the cloud (Hardy et al., 2017).

The use of federated learning has proven effective in identifying high-risk churn groups. Devices with usage decline, increased complaints, or reduced data activity can be flagged locally, with only anonymized signals used in the global model. This approach improves retention efforts while maintaining GDPR-compliant personalization.

5.4. Smart Cities and Massive IoT Integration

The transition to 5G and 6G is enabling the rise of smart cities, where connected devices regulate energy, transportation, environmental monitoring, and public safety. These IoT systems generate massive, decentralized, and often sensitive datasets. Federated learning plays a critical role in managing these ecosystems, particularly when data from sensors, streetlights, surveillance systems, and autonomous vehicles must be processed at the edge.

Consider a smart grid where energy consumption patterns from different neighborhoods are locally analyzed to predict power demand. Instead of transmitting energy logs to a central server, edge nodes compute usage models that can anticipate peak hours, detect equipment faults, or optimize energy distribution. Federated learning ensures that residential privacy is preserved, especially in scenarios involving smart meters and home automation data (Savazzi et al., 2020).

Similarly, autonomous traffic systems benefit from FL by allowing each connected vehicle or road sensor to contribute to a shared understanding of traffic flow, obstacle detection, and routing decisions. These contributions enhance urban traffic optimization without compromising the identity or location history of drivers.

Graphical representations here might include a city-wide map of IoT devices contributing to FL models and a performance comparison between centralized AI and FL in terms of processing time and data privacy.

5.5. Future Directions in Federated Learning for Telecom

The future of federated learning in telecom systems is shaped by advancements in three primary domains: autonomy, adaptability, and auditability.

First, autonomous federated systems are being developed where FL agents can operate with minimal human oversight. These agents would manage training, aggregation, and error correction dynamically, leveraging reinforcement learning and self-healing protocols. This is particularly relevant in telecom networks with fluctuating device availability and shifting user contexts.

Second, FL is moving toward adaptive personalization, where global models are customized for different device clusters or geographical regions. Researchers are exploring *meta-federated learning*, where models not only learn from distributed data but also learn how to learn better across different distributions (Fallah et al., 2020). This approach is expected to revolutionize FL's utility in multicultural, multi-regulatory telecom environments.

Third, the integration of blockchain with federated learning is receiving growing interest, especially for use cases requiring immutable audit trails and decentralized governance. In multi-operator scenarios, blockchain ensures that no single party controls the model or the data flow. Combined with FL, this can enable transparent collaboration between telecom operators, cloud providers, and regulators (Lu et al., 2020).

Emerging FL systems are also being designed to be explainable, using techniques from interpretable machine learning to help operators and regulators understand model decisions. This is particularly important for AI systems involved in credit scoring, fraud flagging, or service denial—where accountability is crucial.

Finally, telecom networks are experimenting with federated reinforcement learning (FRL) for dynamic environments. Unlike supervised FL, FRL enables agents (such as network controllers or base stations) to learn policies by interacting with their environment. These decentralized agents can cooperate to manage spectrum allocation, load balancing, or handover strategies more effectively (Zhang et al., 2021).

6. Conclusion

As data privacy concerns intensify in the era of 5G, AI, and ubiquitous connectivity, the intersection of cloud-telecom convergence and privacy-aware artificial intelligence is becoming both an operational necessity and a strategic imperative. This chapter presents a holistic synthesis of insights discussed in this review, offering a concluding examination of the state, significance, and future of federated learning (FL) as a secure framework for data sharing in next-generation telecom networks.

6.1. Revisiting the Privacy-AI-Telecom Triangle

The integration of AI in telecom infrastructures brings unparalleled value in terms of network intelligence, operational automation, and customer personalization. Yet, this capability is inextricably linked to sensitive user data—voice, location, app usage, billing histories—which are subject to stringent regulatory oversight and public scrutiny (Kairouz et al., 2021). Simultaneously, the shift toward cloud-native telecom infrastructures, such as multi-access edge computing (MEC) and virtualized core networks, compounds the exposure risk by expanding the attack surface.

Federated learning emerges as a compelling response to this triad of concerns. Its privacy-preserving architecture enables the training of AI models across distributed data sources without transferring the underlying data. In doing so, FL supports telecom providers in maintaining regulatory compliance (e.g., with GDPR, CCPA, PIPL), minimizing the risk of data exposure, and enhancing trust with customers and partners (Zhang & Wang, 2020).

6.2. Achievements of Federated Learning in Telecom Contexts

Throughout this review, it has been demonstrated that FL is not just a theoretical abstraction but a practical enabler of multiple mission-critical use cases in telecom environments. From predictive maintenance to fraud detection, and from traffic forecasting to personalized services, FL has proven its value in managing decentralized, sensitive, and voluminous datasets (Liu et al., 2020).

One of the most significant achievements of FL in telecom is its ability to scale personalization while preserving user privacy. Telecom providers can now understand customer needs more granularly—without centralizing behavioral data—thus fostering both operational efficiency and ethical AI.

In addition, FL has shown promise in enhancing inter-operator collaboration. For example, telecom operators operating in different countries can collaborate on improving fraud detection models or network optimization strategies, without ever exchanging raw customer data. This is particularly useful in federations like the GSMA or multi-national telecom conglomerates.

6.3. Persisting Limitations and Operational Trade-offs

Despite these advancements, several operational and technical limitations of FL remain unresolved. Chief among them is the challenge of data heterogeneity, as discussed earlier. Differences in device usage patterns, hardware capabilities, and data quality across telecom nodes continue to impact the performance and convergence speed of federated models (Li et al., 2020).

Additionally, FL introduces considerable infrastructure overhead. The need to deploy orchestration services, secure aggregation protocols, and device management layers places a resource burden on telecom providers, especially those with legacy infrastructure. Moreover, FL does not eliminate the need for centralized monitoring. Instead, it shifts the focus toward monitoring models rather than data, creating a need for new tools and metrics.

From a business perspective, return on investment (ROI) for FL deployments in telecom remains context-specific. In high-margin domains like enterprise 5G or private networks, FL may offer clear cost-to-benefit ratios. But in consumer telecom, where ARPU (Average Revenue Per User) is declining, the economic case for FL requires more robust validation through longitudinal deployments.

6.4. Future Research and Policy Implications

Looking ahead, FL's role in the telecom sector is expected to deepen, especially as networks become hyper-distributed with 6G, satellite backhauls, and AI-native architectures. However, for FL to reach its full potential, several avenues for future research must be pursued.

First, there is a growing need for explainable federated learning. In sensitive applications such as credit scoring or fraud flagging, regulators and stakeholders require insight into how decisions are made by AI systems. Future FL systems must integrate explainability into their pipelines to ensure transparency and accountability (Fallah et al., 2020).

Second, energy-efficient FL will be critical. With thousands or millions of edge devices participating in training, energy consumption becomes a serious environmental and economic issue. Research into lightweight FL algorithms, edge-aware pruning, and selective participation models will be essential.

Third, policy frameworks must evolve to accommodate decentralized AI. Current data protection laws focus primarily on centralized data controllers and processors. FL introduces a new paradigm where multiple actors contribute to a shared model without sharing data. Policymakers must redefine roles, responsibilities, and liability boundaries in this emerging landscape (Zhang et al., 2021).

6.5. Final Reflections

In conclusion, federated learning represents a paradigm shift in how artificial intelligence is deployed within cloud-telecom infrastructures. By redefining the relationship between data utility and privacy, FL allows telecom operators to transform their networks into intelligent, responsive, and secure ecosystems.

This review argues that FL is not a panacea but a pivotal layer in the privacy-aware AI stack. When integrated with complementary technologies—such as edge computing, differential privacy, and blockchain—FL can unlock new business models, from autonomous network management to privacy-preserving partnerships across operators and verticals.

The telecom industry stands at a critical juncture. As digital demands rise and privacy regulations tighten, the adoption of federated learning could determine whether networks evolve into trusted platforms—or remain mere data pipes. The path ahead requires technical innovation, regulatory modernization, and cross-sector collaboration. But the trajectory is clear: privacy-aware, federated intelligence will be foundational to the next generation of cloud-telecom convergence.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., & Zhang, L. (2016). Deep learning with differential privacy. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 308–318. https://doi.org/10.1145/2976749.2978318

[2] Bagdasaryan, E., Veit, A., Hua, Y., Estrin, D., & Shmatikov, V. (2020). How to backdoor federated learning. Proceedings of the 23rd International Conference on Artificial Intelligence and Statistics (AISTATS), 2938–2948. https://arxiv.org/abs/2007.09626

[3] Blanchard, P., El Mhamdi, E. M., Guerraoui, R., & Stainer, J. (2017). Machine learning with adversaries: Byzantine tolerant gradient descent. Advances in Neural Information Processing Systems, 119–129. https://arxiv.org/abs/1705.09071

[4] Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., ... & Seth, K. (2017). Practical secure aggregation for privacy-preserving machine learning. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 1175–1191. https://doi.org/10.1145/3133956.3134000

[5] Olufemi, O. D., Ikwuogu, O. F., Kamau, E., Oladejo, A. O., Adewa, A., & Oguntokun, O. (2024). Infrastructure-as-code for 5g ran, core and sbi deployment: a comprehensive review. International Journal of Science and Research Archive, 21(3), 144-167. https://doi.org/10.30574/gjeta.2024.21.3.0235

[6] Caldas, S., Wu, P., Li, T., Konečnỳ, J., McMahan, H. B., Smith, V., & Talwalkar, A. (2019). LEAF: A benchmark for federated settings. arXiv preprint arXiv:1812.01097. https://arxiv.org/abs/1812.01097

[7] Chen, Z., & Liu, B. (2018). Lifelong machine learning. Synthesis Lectures on Artificial Intelligence and Machine Learning, 12(3), 1–207. https://doi.org/10.2200/S00832ED1V01Y201804AIM037

[8] Fallah, A., Mokhtari, A., & Ozdaglar, A. (2020). Personalized federated learning: A meta-learning approach. Advances in Neural Information Processing Systems (NeurIPS), 33, 6966–6978. https://arxiv.org/abs/2003.01503

[9] Gentry, C. (2009). A fully homomorphic encryption scheme. Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC), 169–178. https://doi.org/10.1145/1536414.1536440

[10] Ghosh, A., & Gupta, R. (2021). Federated learning in telecommunication systems: A survey. IEEE Access, 9, 92704–92716. https://doi.org/10.1109/ACCESS.2021.3096268

[11] Hardy, S., Henecka, W., Ivey-Law, H., Nock, R., Patrini, G., Smith, G., & Thorne, B. (2017). Private federated learning on vertically partitioned data via entity resolution and additively homomorphic encryption. arXiv preprint arXiv:1711.10677. https://arxiv.org/abs/1711.10677

[12] Kairouz, P., McMahan, H. B., et al. (2021). Advances and open problems in federated learning. Foundations and Trends® in Machine Learning, 14(1–2), 1–210. https://doi.org/10.1561/2200000083

[13] Olufemi, O. D., Ikwuogu, O. F., Kamau, E., Oladejo, A. O., Adewa, A., & Oguntokun, O. (2024). Infrastructure-as-code for 5g ran, core and sbi deployment: a comprehensive review. International Journal of Science and Research Archive, 21(3), 144-167. https://doi.org/10.30574/gjeta.2024.21.3.0235

[14] Liu, Y., Kang, J., Niyato, D., & Zhang, Y. (2020). A secure federated learning framework for 5G-enabled vehicular networks. IEEE Transactions on Vehicular Technology, 69(5), 4960–4972. https://doi.org/10.1109/TVT.2020.2982517

[15] Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated optimization in heterogeneous networks. Proceedings of Machine Learning and Systems, 2, 429–450. https://proceedings.mlsys.org/paper/2020/file/48a470dcb292f1bdf8c0b1b4c0f2c945-Paper.pdf

[16] Li, X., Li, Q., & Li, H. (2020). Privacy-preserving machine learning in the cloud. IEEE Transactions on Knowledge and Data Engineering, 32(3), 423-436. https://doi.org/10.1109/TKDE.2019.2910398

[17] Liu, Z., Xu, T., & Li, H. (2020). Secure federated learning with differential privacy. IEEE Transactions on Cybernetics, 50(12), 4777–4789. https://doi.org/10.1109/TCYB.2020.2993523

[18] Bobie-Ansah, D., Olufemi, D., & Agyekum, E. K. (2024). Adopting infrastructure as code as a cloud security framework for fostering an environment of trust and openness to technological innovation among businesses: Comprehensive review. International Journal of Science & Engineering Development Research, 9(8), 168–183. http://www.ijrti.org/papers/IJRTI2408026.pdf

[19] McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, 1273–1282. https://proceedings.mlr.press/v54/mcmahan17a.html

[20] Nishio, T., & Yonetani, R. (2019). Client selection for federated learning with heterogeneous resources in mobile edge. IEEE International Conference on Communications (ICC), 1–7. https://doi.org/10.1109/ICC.2019.8761707

[21] Nock, R., & Smith, G. (2020). Privacy-preserving machine learning in cloud environments. IEEE Transactions on Cloud Computing, 8(2), 200–210. https://doi.org/10.1109/TCC.2019.2910258

[22] Savazzi, S., Nicoli, M., Bennis, M., & Kianoush, S. (2020). Opportunistic edge computing for IoT: When the cloud meets the swarm. EURASIP Journal on Wireless Communications and Networking, 2020(1), 1–19. https://doi.org/10.1186/s13638-020-1931-x

[23] Olufemi, O. D., Ejiade, A. O., Ogunjimi, O., & Ikwuogu, F. O. (2024). AI-enhanced predictive maintenance systems for critical infrastructure: Cloud-native architectures approach. World Journal of Advanced Engineering Technology and Sciences, 13(02), 229–257. https://doi.org/10.30574/wjaets.2024.13.2.0552

[24] Sattler, F., Wiedemann, S., & Müller, K. (2020). Federated learning for non-iid data: A perspective on distributed optimization. Proceedings of the 2020 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 345–354. https://arxiv.org/abs/2006.12381

[25] Sun, B., & Yang, H. (2019). Federated learning with imbalanced data for telecom. IEEE Transactions on Network and Service Management, 16(2), 168–179. https://doi.org/10.1109/TNSM.2019.2890816

[26] Zhao, Y., Li, M., Lai, L., & Song, S. (2018). Federated learning with non-IID data via local class imbalance learning. arXiv preprint arXiv:1806.00582. https://arxiv.org/abs/1806.00582

[27] Zhang, Q., & Wang, Z. (2020). Federated learning for privacy-preserving AI in 5G. IEEE Wireless Communications, 27(6), 88–94. https://doi.org/10.1109/MWC.001.1900327

[28] Zhang, Y., Zhang, L., & Xu, X. (2021). Edge computing and federated learning for privacy-preserving AI. IEEE Network, 35(4), 58–64. https://doi.org/10.1109/MNET.010.2000501

[29] Zhu, L., Liu, Z., & Han, S. (2019). Deep leakage from gradients. Advances in Neural Information Processing Systems (NeurIPS), 32, 2662–2671. https://arxiv.org/abs/1811.09450

[30] Yurochkin, M., Agarwal, M., Ghosh, S., Greenewald, K., & Khazaeni, Y. (2019). Bayesian nonparametric federated learning of neural networks. Proceedings of the 36th International Conference on Machine Learning (ICML), 2790–2800. https://arxiv.org/abs/1903.08487

[31] David Olufemi, Ayodeji Olutosin Ejiade, Friday Ogochukwu Ikwuogu, Phebe Eleojo Olufemi, Deligent Bobie-Ansah, 2025, Securing Software-Defined Networks (SDN) Against Emerging Cyber Threats in 5G and Future Networks – A Comprehensive Review, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 14, Issue 02 (February 2025).

[32] Nishio, T., & Yonetani, R. (2019). Client selection for federated learning with heterogeneous resources in mobile edge. IEEE International Conference on Communications (ICC), 1–7. https://doi.org/10.1109/ICC.2019.8761707

[33] Fallah, A., Mokhtari, A., & Ozdaglar, A. (2020). Personalized federated learning: A meta-learning approach. Advances in Neural Information Processing Systems (NeurIPS), 33, 6966–6978.

[34] Hardy, S., Henecka, W., Ivey-Law, H., Nock, R., Patrini, G., Smith, G., & Thorne, B. (2017). Private federated learning on vertically partitioned data via entity resolution and additively homomorphic encryption. arXiv preprint arXiv:1711.10677.

[35] McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. Proceedings of the 20th International Conference on Artificial Intelligence and Statistics.

[36] Li, X., Li, Q., & Li, H. (2020). Privacy-preserving machine learning in the cloud. IEEE Transactions on Knowledge and Data Engineering.

[37] Ghosh, A., & Gupta, R. (2021). Federated learning in telecommunication systems: A survey. IEEE Access.

[38] Zhang, Y., Zhang, L., & Xu, X. (2021). Edge computing and federated learning for privacy-preserving AI. IEEE Network.

[39] Kairouz, P., McMahan, H. B., et al. (2021). Advances and open problems in federated learning. Foundations and Trends® in Machine Learning, 14(1–2), 1–210.

[40] Zhang, Y., Zhang, L., & Xu, X. (2020). Federated learning in 5G: A review. IEEE Wireless Communications, 27(6).

[41] Adewa, A., Anyah, V., Olufemi, O. D., Oladejo, A. O., & Olaifa, T. (2025). The impact of intent-based networking on network configuration management and security. Global Journal of Engineering and Technology Advances, 22(01), 063-068. https://doi.org/10.30574/gjeta.2025.22.1.0012

[42] Zhang, Q., & Wang, Z. (2020). Federated learning for privacy-preserving AI in 5G. IEEE Wireless Communications.

[43] Savazzi, S., Nicoli, M., Bennis, M., & Kianoush, S. (2020). Opportunistic edge computing for IoT: When the cloud meets the swarm. EURASIP Journal on Wireless Communications and Networking, 2020(1).

[44] Fallah, A., Mokhtari, A., & Ozdaglar, A. (2020). Personalized federated learning: A meta-learning approach. Advances in Neural Information Processing Systems.

[45] Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated optimization in heterogeneous networks. Proceedings of Machine Learning and Systems, 2, 429–450.

[46] Zhao, Y., Li, M., Lai, L., & Song, S. (2020). Federated learning for privacy-preserving AI in 5G. IEEE Wireless Communications, 27(6), 88–94.

[47] Bobie-Ansah, D., & Affram, H. (2024). Impact of secure cloud computing solutions on encouraging small and medium enterprises to participate more actively in e-commerce. International Journal of Science & Engineering Development Research, 9(7), 469–483. http://www.ijrti.org/papers/IJRTI2407064.pdf

[48] Yurochkin, M., Agarwal, M., Ghosh, S., Greenewald, K., & Khazaeni, Y. (2020). Bayesian nonparametric federated learning of neural networks. Proceedings of the 36th International Conference on Machine Learning (ICML), 2790–2800.

[49] Fallah, A., Mokhtari, A., & Ozdaglar, A. (2020). Personalized federated learning: A meta-learning approach. NeurIPS 2020.

[50] Liu, Y., Kang, J., Niyato, D., & Zhang, Y. (2020). A secure federated learning framework for 5G-enabled vehicular networks. IEEE Transactions on Vehicular Technology.

[51] Nishio, T., & Yonetani, R. (2019). Client selection for federated learning with heterogeneous resources in mobile edge. IEEE International Conference on Communications (ICC), 1–7.

[52] McMahan, B., Moore, E., Ramage, D., & Hampson, S. (2017). Communication-efficient learning of deep networks from decentralized data. Proceedings of the 20th International Conference on Artificial Intelligence and Statistics.

[53] Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated optimization in heterogeneous networks. Proceedings of Machine Learning and Systems.

[54] Zhang, Q., & Wang, Z. (2020). Federated learning for privacy-preserving AI in 5G. IEEE Wireless Communications, 27(6).

[55] Zhang, Y., Zhang, L., & Xu, X. (2021). Edge computing and federated learning for privacy-preserving AI. IEEE Network.