Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Caleb et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

Federated Learning Techniques for Privacy-Preserving AI in Distributed Networks: A Review

Research Article https://stem.techspherejournal.com

Article Info
Revised Date: 18th October 2025
Accepted Date: 26th October 2025
Published Date: 31st October 2025

Keywords
Federated Learning
Privacy-Preserving Artificial Intelligence
Differential Privacy
Homomorphic Encryption
Distributed Machine Learning

Author Details
Akinsiku Ayokunle Michael
Department of Computer Science, The Federal Polytechnic Ado-Ekiti, Ekiti State, Nigeria.
****Corresponding author's email***: akinsiku_am@fedpolyado.edu.ng
DOI: **https://doi.org/10.5281/zenodo.17496759**

ABSTRACT

Federated Learning (FL) represents a transformative paradigm in artificial intelligence (AI), designed to enable decentralized model training across distributed data sources without requiring the direct exchange of raw data. Unlike traditional centralized learning approaches that aggregate datasets in a single location, often raising privacy, security, and compliance concerns, FL allows multiple clients, such as mobile devices, edge nodes, or institutional servers, to collaboratively train a shared global model while preserving local data confidentiality. This decentralized approach has made FL a key enabler of privacy-preserving AI, particularly in sensitive domains such as healthcare, finance, and industrial automation. This paper provides a comprehensive exploration of privacy-preserving mechanisms within federated learning, focusing on techniques such as Differential Privacy (DP), Homomorphic Encryption (HE), Secure Multi-Party Computation (SMPC), and blockchain-based frameworks. It further examines communication efficiency and system optimization strategies, including model compression, adaptive aggregation, and energy-efficient computation for resource-constrained devices. The study also highlights real-world applications of FL in Internet of Things (IoT), smart cities, and biomedical data analysis, showcasing its versatility across diverse distributed environments. Additionally, key challenges, such as data heterogeneity, scalability, and security vulnerabilities, are analyzed alongside a comparative assessment of leading FL algorithms and privacy techniques. Ultimately, this paper underscores how federated learning bridges the gap between high-performance AI and stringent data privacy requirements, presenting future research directions for robust, transparent, and privacy-enhanced intelligent systems.

1 Introduction

1.1 Background and Motivation

The proliferation of connected devices and distributed data sources such as the Internet of Things (IoT), edge devices, and mobile networks has led to an exponential increase in the amount of data generated at the network edge. This data, produced continuously by sensors, smartphones, and other smart devices, presents a valuable resource for training intelligent systems capable of supporting personalized, context-aware services. However, traditional artificial intelligence (AI) and machine learning (ML) approaches typically rely on centralized data collection and processing, which necessitate aggregating raw data from multiple sources into a central server or cloud for model training [1].

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Caleb et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

While centralization facilitates computational efficiency and model accuracy, it raises significant concerns regarding data privacy, ownership, and regulatory compliance. Sensitive data—such as personal health records, financial information, and user behavioral data, may be exposed to breaches or unauthorized access during collection, transmission, or storage. Moreover, the centralization paradigm conflicts with stringent data protection frameworks such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), both of which emphasize user consent and data minimization principles [2].

To address these privacy and data security challenges, Federated Learning (FL) has emerged as a transformative paradigm for distributed AI model training. FL enables multiple clients or devices to collaboratively train a shared global model without transferring their raw data to a central repository [3]. Instead, only model parameters or gradients are exchanged with an aggregation server, ensuring that data remains localized on individual devices. This architecture provides a robust foundation for privacy-preserving AI, allowing organizations and individuals to benefit from collective intelligence while maintaining strict data confidentiality.

1.2 Problem Statement

Despite the growing adoption of Federated Learning, achieving an optimal balance between model performance and data privacy remains an open challenge. Federated systems often encounter issues related to communication efficiency, model convergence, and data heterogeneity across clients. Moreover, existing centralized AI models, and even some FL implementations, remain vulnerable to privacy leakage through gradient inversion, model poisoning, and inference attacks [4].

These vulnerabilities compromise both model integrity and user trust. Additionally, current privacy-preserving techniques such as differential privacy, homomorphic encryption, and secure multi-party computation introduce trade-offs in computational cost, communication overhead, and accuracy. Consequently, a comprehensive review of existing FL approaches is required to assess their strengths, limitations, and applicability in diverse distributed environments.

1.3 Research Questions

This paper aims to provide a comprehensive review of federated learning techniques for privacy-preserving AI in distributed networks. The specific objectives are as follows:

1. To examine existing federated learning architectures and algorithms that enhance data privacy while maintaining model utility.
2. To evaluate privacy-preserving mechanisms, such as differential privacy, homomorphic encryption, and secure aggregation, used within federated environments.
3. To analyze practical applications of federated learning across domains such as IoT, healthcare, finance, and smart infrastructure.
4. To identify open challenges, research gaps, and future directions for developing efficient and scalable privacy-preserving FL systems.

1.4 Scope and Significance

The scope of this review encompasses federated learning implementations and privacy-preserving strategies applied in distributed networks, including Internet of Things (IoT) systems, mobile edge computing, and healthcare environments. The paper also discusses algorithmic improvements that reduce communication cost, address data heterogeneity, and enhance security in federated systems.

The significance of this study lies in its contribution to understanding how FL can serve as a privacy-centric alternative to conventional AI frameworks. As global data regulations such as GDPR (Europe) and HIPAA (United States) continue to enforce stricter controls over personal data handling, privacy-preserving AI approaches are becoming essential for compliance and user trust. Federated Learning, therefore, represents a vital enabler for secure, collaborative intelligence in modern distributed systems.

2 Conceptual Framework of Federated Learning

2.1 Definition and Basic Architecture

Federated Learning (FL) is a distributed machine learning paradigm that enables multiple clients, such as mobile devices, edge servers, or organizations, to collaboratively train a shared global model without exchanging their local raw data [5]. Instead of centralizing data on a single server, FL keeps data decentralized and transfers only model parameters or gradients for aggregation. This approach preserves data privacy while still benefiting from the collective intelligence of multiple participants [6].
The federated learning process typically involves three main phases:

a. **Local Training:**
Each client downloads the current global model from the central coordinating server. Using its local dataset, the client performs several iterations of model training to update the model weights. Since data never leaves the device, privacy is maintained [5].

b. **Model Aggregation:**
After local training, each client sends the updated model parameters (not raw data) to the server. The server aggregates these updates using an algorithm such as Federated Averaging (FedAvg) to produce an improved global model [7].

c. **Global Model Update:**
The aggregated model is redistributed to all clients, replacing the previous version. The cycle of local training and global aggregation continues iteratively until convergence is achieved [8].

Key Components of a Federated Learning System include:

1. **Clients (or Participants):** Devices or institutions that hold local datasets and perform training operations.
2. **Central Server (Aggregator):** Coordinates the training process, receives local updates, aggregates them, and distributes the updated model.
3. **Model Parameters:** Numerical weights and biases that represent the learned knowledge of the model, which are periodically exchanged between clients and server.
4. **Communication Channel:** The network infrastructure enabling secure transfer of model parameters.
5. **Privacy-Preserving Layer:** Mechanisms such as encryption, differential privacy, or secure aggregation that protect sensitive data during communication.

The architecture can be mathematically expressed as:

$$w_{t+1} = \sum_{k=1}^{K} \frac{n_k}{N} w_{t+1}^{k} \quad (1)$$

where w_{t+1} is the aggregated global model, w_{t+1}^{k} is the local model of the client k n_k is the number of samples on client k, and N is the total number of samples across all clients [8].

2.2 Types of Federated Learning

Depending on the data distribution and feature alignment among participating clients, federated learning is typically categorized into three major types: Horizontal Federated Learning (HFL), Vertical Federated Learning (VFL), and Federated Transfer Learning (FTL) [9].

2.2.1 Horizontal Federated Learning (HFL)

In HFL, also known as sample-based federated learning, the datasets across different clients share the same feature space but contain different samples or user records. For example, multiple hospitals collecting the same set of patient

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Caleb et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

attributes (e.g., age, blood pressure, diagnosis) but serving different patient populations can collaboratively train a shared model without sharing raw data.
This type of FL is the most common and forms the foundation of many modern applications such as mobile keyboard prediction and IoT device learning [10].

2.2.2 Federated Transfer Learning (FTL)

VFL, or feature-based federated learning, involves clients that possess datasets with overlapping user samples but different feature spaces. For instance, a bank and an e-commerce company may have information about the same customers but store different attributes, financial transactions versus purchasing preferences.
In such scenarios, federated learning allows joint model training through encrypted feature alignment while maintaining data confidentiality [11].

2.2.3 Vertical Federated Learning (VFL)

FTL extends federated learning to situations where both the feature space and the sample space are partially overlapping. This approach leverages transfer learning to transfer knowledge from one domain (source) to another (target) with minimal shared data. FTL is particularly useful when participating clients have small, heterogeneous datasets or when cross-domain adaptation is required [12].
Through domain adaptation techniques and representation learning, FTL enhances model generalization while still preserving privacy.

2.3 Comparison with Centralized and Decentralized Learning

Federated Learning represents a hybrid paradigm that differs substantially from both centralized and fully decentralized (peer-to-peer) learning systems in terms of architecture, data flow, and privacy protection [13].

Aspect	Centralized Learning	Federated Learning	Decentralized Learning
Data Location	All data is collected and stored in a central server.	Data remains on client devices; only model updates are shared.	No central server; peers exchange updates directly.
Privacy Level	Low, raw data is exposed to central entities.	High—data never leaves local devices.	High, no data centralization, but synchronization is complex.
Architecture	Centralized server-client model.	Semi-centralized with a coordinating aggregation server.	Fully distributed with peer-to-peer communication.
Communication Pattern	One-way data upload.	Two-way model exchange (upload and download).	Multi-way, requiring consensus protocols.
Security Risks	Data breaches at central server.	Gradient leakage, poisoning attacks.	Network instability, trust management issues.
Examples	Cloud-based AI training.	Google's Gboard, healthcare FL systems.	Blockchain-based machine learning.

3 Privacy-Preserving Mechanisms in Federated Learning

Federated Learning (FL) provides a decentralized model training framework that inherently enhances data privacy by keeping raw data local to client devices. However, the exchange of model parameters or gradients between clients and the central server can still expose sensitive information through indirect inference or gradient inversion attacks [14]. To address these vulnerabilities, several privacy-preserving techniques have been developed to strengthen FL systems against data leakage and adversarial manipulation. This section discusses key mechanisms including Differential Privacy

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Caleb et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

(DP), Homomorphic Encryption (HE), Secure Multi-Party Computation (SMPC), Blockchain-enabled FL, and Hybrid Approaches.

3.1 Differential Privacy (DP)

Differential Privacy is a formal mathematical framework that ensures the output of a computation does not significantly change when any single record in the dataset is altered or removed [15]. In the context of federated learning, DP helps prevent information leakage from model updates by adding controlled noise to gradients or model parameters before they are shared with the central aggregator. This noise makes it computationally difficult for an adversary to infer any individual's data contribution.

3.1.1 Mathematical Formulation

A randomized algorithm A satisfies (ε, δ)-differential privacy if, for all datasets D_1 and D_2 differing by at most one record, and for all possible outputs S:

$$P[A(D_1) \in S] \leq e^{\varepsilon}.P[A(D_2)\epsilon\, S] + \delta \quad \text{.....(2)}$$

Here:

- ε (epsilon) controls the privacy loss — smaller values mean stronger privacy.
- δ represents the probability that the privacy guarantee fails.

In FL, noise sampled from a Gaussian or Laplacian distribution is often added to the model gradients or parameter updates before they are uploaded to the central server. The Federated Averaging with Differential Privacy (FedAvg-DP) approach is widely used to achieve a balance between privacy preservation and model utility [16].

3.1.2 Advanced Extortion (2021–2025): AI-Assisted and LOTL Techniques

While LOTL tactics employed legitimate technologies such as PowerShell and PsExec, attackers leveraged AI for spear-phishing and evasion [17], [18]. It was documented that the use of privacy coins and mixers for Bitcoin laundering. National-level repercussions were best illustrated by the Colonial Pipeline attack in 2021 [19].

3.1.3 Use Cases in FL

a. **Healthcare Systems:** DP is applied to medical data sharing scenarios where patient privacy is critical [20].
b. **Mobile Applications:** Used in federated recommendation and keyboard prediction systems such as Google's Gboard [21].
c. **IoT Devices:** Ensures that device-level data patterns are not reverse-engineered through model updates [22].

DP remains a cornerstone of privacy-preserving FL due to its rigorous mathematical guarantees, though it often introduces a trade-off between privacy strength and model accuracy.

3.2 Homomorphic Encryption (HE)

Homomorphic Encryption (HE) is a cryptographic technique that allows computations to be performed directly on encrypted data without requiring decryption. This enables the aggregation of encrypted model updates in federated learning systems, ensuring that sensitive data remains confidential even during processing [23].

3.2.1 Encryption-Based Aggregation

In an HE-enabled FL system, each client encrypts its local model parameters or gradients using a shared public key before transmitting them to the central aggregator [24]. The server then performs aggregation operations (e.g., summation or averaging) on the encrypted data. The aggregated result can only be decrypted using the corresponding private key, which is held securely by the clients or a trusted third party.

Mathematically, given an encryption function E and decryption function D:

$$E(w_1) \oplus E(w_2) = E(w_1 + w_2) \quad \text{.....(3)}$$

and

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Caleb et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

$$D\big(E(w_1 + w_2)\big) = w_1 + w_2 \quad \text{.....(4)}$$

This property allows secure summation or averaging of model parameters without exposing individual contributions.

3.2.2 Use Cases in FL

a. Financial Networks: HE ensures the confidentiality of sensitive transaction data during federated credit scoring.
b. Cross-Institutional Collaborations: Hospitals and research institutions use HE-based FL to train shared diagnostic models securely [25].

While HE provides strong cryptographic protection, it increases computational complexity and communication overhead, which can be mitigated through lightweight or partial homomorphic schemes

3.3 Secure Multi-Party Computation (SMPC)

Secure Multi-Party Computation (SMPC) allows multiple participants to jointly compute a function over their inputs while keeping each input private [26]. In federated learning, SMPC enables clients to collaboratively train a model such that no party, including the central server, learns the raw model updates of any other participant.

3.3.1 Collaborative Learning without Direct Data Exposure

The basic idea behind SMPC is to split each client's model parameters into multiple encrypted "shares," which are distributed among different parties. These shares are then aggregated securely without revealing the underlying data. After aggregation, the final model is reconstructed without exposing any individual's update.
For instance, given two clients A and B:

a. A holds model update w_A, B holds w_B.
b. Each splits its data into secret shares and exchanges them.
c. Aggregation occurs via an additive secret sharing protocol to compute $w = w_a + w_B$ securely.

SMPC ensures confidentiality even if some participants are semi-honest (i.e., follow protocol but attempt to infer information). However, scalability and communication latency remain ongoing challenges.

Applications

a. Healthcare Consortia: Collaborative disease prediction models.
b. Multi-Bank Fraud Detection: Secure joint model training across different banks without revealing customer data.

3.4 Blockchain-Enabled Federated Learning

Blockchain technology has recently been integrated into federated learning systems to enhance trust, transparency, and decentralization [27]. By leveraging blockchain's distributed ledger, FL participants can verify the integrity of model updates and eliminate reliance on a single central aggregator.

3.4.1 Role in Federated Learning

1. **Transparency and Traceability:**
   Every model update and aggregation event is recorded on the blockchain ledger, ensuring traceability of training contributions.
2. **Security and Integrity:**
   The immutability of blockchain prevents malicious modification of model updates. Consensus mechanisms (e.g., Proof-of-Stake or Practical Byzantine Fault Tolerance) ensure secure agreement among participants.
3. **Incentive Mechanisms:**
   Blockchain can facilitate token-based incentives or reputation systems to reward honest participation and penalize malicious behavior.
4. **Decentralized Model Management:**

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Caleb et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

Smart contracts can automate aggregation, validation, and reward distribution without centralized control.

Applications

a. **Smart Cities:** Secure coordination of data from distributed IoT sensors.
b. **Autonomous Vehicles:** Decentralized learning of navigation models among vehicles and road infrastructure.

Despite its potential, blockchain integration introduces latency and energy consumption challenges, especially in large-scale systems.

3.5 Hybrid and Emerging Techniques

Recent research trends combine multiple privacy-preserving mechanisms to create robust and adaptive FL frameworks that address both data confidentiality and system efficiency.

Hybrid Approaches

a. DP + HE: Noise is added to model updates (DP) before encrypting them (HE) to achieve dual-layer protection [28].
b. Blockchain + SMPC: Blockchain ensures auditability and trust, while SMPC secures the aggregation process.
c. DP + Blockchain: Differentially private updates are recorded on blockchain for verifiable and privacy-safe learning history.

Emerging Trends

a. Federated Trusted Execution Environments (TEE): Hardware-based secure enclaves for isolated computation.
b. Post-Quantum Secure FL: Algorithms resistant to attacks from quantum computers.
c. Adaptive Privacy Budgets: Dynamic adjustment of DP parameters based on model sensitivity and data characteristics.

Hybrid frameworks demonstrate that no single privacy technique suffices for all FL scenarios. Combining multiple methods provides layered security, improved robustness, and better compliance with global privacy standards.

4 Communication Efficiency and System Optimization

Efficient communication and resource utilization are among the most critical factors influencing the scalability and practicality of federated learning (FL) systems. As FL involves frequent exchanges of model parameters or gradients between multiple clients and a central server, it introduces significant communication overhead, latency, and energy consumption, particularly in resource-constrained environments like mobile or IoT devices. To address these challenges, several strategies have been developed to enhance communication efficiency and optimize the overall system performance.

4.1 Model Compression and Parameter Quantization

Model compression techniques aim to reduce the size of transmitted updates without significantly compromising model accuracy. By minimizing the volume of data exchanged between clients and the server, these methods help alleviate network congestion and lower communication costs [29].

Parameter quantization reduces the precision of model weights and gradients (e.g., from 32-bit floating-point to 8-bit or lower representations), thereby decreasing transmission bandwidth requirements. Sparsification further enhances efficiency by only transmitting significant or non-zero updates while pruning redundant parameters. Other compression strategies, such as knowledge distillation and low-rank factorization, are also employed to reduce the computational burden during local training.

For instance, algorithms like Deep Gradient Compression (DGC) and Top-k Gradient Sparsification have been shown to reduce communication loads by more than 90% while maintaining comparable model performance [30]. These techniques are especially beneficial for large-scale federated systems deployed across heterogeneous networks.

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Caleb et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

4.2 Adaptive Aggregation and Client Selection

The heterogeneity of clients, stemming from variations in computational power, network bandwidth, and data quality, necessitates adaptive mechanisms for model aggregation and client participation [31]. Instead of uniformly aggregating updates from all clients, adaptive aggregation techniques weigh client contributions based on reliability, update frequency, or data representativeness.

Federated Averaging (FedAvg) remains the most commonly used aggregation algorithm, but its static approach can be suboptimal for dynamic networks [6]. Enhanced methods such as FedProx, FedNova, and FedDyn introduce adaptive optimization and regularization to improve fairness and convergence stability.

Additionally, client selection strategies, like importance-based or reward-driven selection, reduce unnecessary communication by engaging only a subset of clients with high-quality data or stable connectivity. This approach improves overall efficiency and reduces synchronization delays.

4.3 Asynchronous Federated Learning

Traditional FL assumes synchronous updates, where the central server waits for all clients to complete their local training before aggregating updates. However, this model often leads to stragglers, clients with slower computation or unstable connections, thereby increasing idle times and reducing throughput [32].

Asynchronous Federated Learning (AFL) relaxes this requirement by allowing the server to update the global model as soon as client updates arrive. This approach significantly enhances scalability and responsiveness, especially in large, geographically distributed networks [33].

Nonetheless, AFL introduces challenges in maintaining model consistency, as updates may be based on outdated global models. To mitigate this, staleness-aware aggregation techniques and timestamp-based weighting are used to balance performance and stability. Examples include algorithms like FedAsync and FedBuff, which provide practical frameworks for asynchronous coordination in federated environments.

4.4 Energy-Efficient FL in Resource-Constrained Devices

Energy efficiency is a vital consideration for FL systems deployed on IoT devices, smartphones, or edge sensors with limited power capacity. Repeated local computations and data transmissions can quickly drain battery life, making sustainability a critical design goal [34].

To address this, energy-aware scheduling and resource-adaptive training techniques dynamically adjust local computation intensity, update frequency, and communication intervals based on device conditions [35]. Approaches such as federated dropout, early stopping, and partial model updates minimize redundant computations without compromising accuracy.

Moreover, edge-assisted federated learning, where intermediary edge servers handle aggregation and pre-processing tasks, significantly reduces energy and latency costs. Energy-efficient protocols like E-FedAvg and GreenFL have demonstrated that optimizing both computation and communication workloads can extend device longevity and improve participation rates across networks.

The optimization of communication and system efficiency in federated learning is crucial for enabling large-scale deployment across heterogeneous and distributed environments [10]. Techniques such as model compression, adaptive aggregation, asynchronous coordination, and energy-efficient scheduling collectively ensure scalability, reliability, and sustainability. These mechanisms are foundational to realizing real-world, privacy-preserving AI systems that can operate seamlessly across constrained, decentralized infrastructures.

5 Applications of Federated Learning in Distributed Networks

Federated Learning (FL) has gained significant attention as a transformative paradigm for enabling collaborative intelligence across distributed networks without compromising data privacy. By allowing local devices or institutions to

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Caleb et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

train models on decentralized data and share only model parameters, FL has proven adaptable to multiple domains. The following subsections highlight key real-world applications of FL in various distributed network settings.

5.1 Internet of Things (IoT) and Edge Computing

The Internet of Things (IoT) ecosystem comprises billions of interconnected devices, sensors, cameras, mobile phones, and embedded systems, that continuously generate vast amounts of data [36]. Transmitting this data to centralized servers is both bandwidth-intensive and privacy-risky.

Federated Learning provides a privacy-preserving and bandwidth-efficient alternative by enabling local training directly on edge devices. The aggregated model learns collectively without requiring raw data transmission, thereby minimizing privacy exposure and network congestion.

For example, in smart home systems, FL enables devices such as thermostats, security cameras, and voice assistants to collaboratively improve performance (e.g., predictive maintenance or user behavior modeling) while keeping sensitive user data local. Similarly, edge-assisted federated learning integrates computation at the edge layer, reducing latency and enhancing scalability in applications like real-time object detection, anomaly detection in industrial IoT, and network intrusion detection systems (NIDS) [37].

5.2 Healthcare and Biomedical Data Analysis

Healthcare is among the most privacy-sensitive domains, where data sharing across hospitals, laboratories, and research institutions is heavily regulated by frameworks such as HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation) [38].

Federated Learning offers a secure solution for multi-institutional medical data analysis without violating data protection laws. Hospitals can collaboratively train predictive models on patient records, medical images, or genomic data without disclosing private health information.

Applications include:

a. **Medical imaging:** Collaborative training of deep learning models for disease diagnosis (e.g., tumor detection from MRI scans) across hospitals.
b. **Drug discovery and genomics:** Joint learning on molecular data from different research labs.
c. **Personalized medicine:** Building adaptive models that tailor treatments based on patient demographics and genetic profiles.

Prominent examples include Google's Federated Learning for mobile-based health monitoring, and federated medical imaging frameworks like FedHealth and Federated Tumor Segmentation (FeTS), which have demonstrated improved diagnostic accuracy with enhanced data confidentiality [39].

5.3 Finance and Banking Systems

The financial industry faces unique challenges involving sensitive transactional data, regulatory compliance, and cybersecurity risks. FL provides a means for multiple banks, fintech institutions, or insurance firms to collaboratively train fraud detection or risk assessment models without sharing raw customer data.

For instance, FL enables collaborative anti-money laundering (AML) models that learn from transaction data across institutions, detecting illicit patterns without breaching data confidentiality [40]. Similarly, in credit scoring and customer behavior analysis, FL aggregates insights across distributed financial systems to enhance model robustness and fairness. By integrating privacy-preserving techniques like secure aggregation and differential privacy, FL ensures compliance with regulatory mandates while enhancing security analytics, credit modeling, and algorithmic transparency. Moreover, the use of blockchain-based federated frameworks further enhances auditability and trust among participating financial entities.

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Caleb et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

5.4 Smart Cities and Transportation

The rapid expansion of smart city infrastructure, including connected vehicles, traffic cameras, and environmental sensors, has created massive data networks that require intelligent and privacy-aware coordination. Federated Learning serves as a cornerstone technology for urban analytics and intelligent transportation systems (ITS) by enabling distributed model training across devices deployed throughout a city [41].

In transportation, FL facilitates:

a. **Autonomous vehicle coordination:** Sharing model updates related to driving behavior, obstacle detection, and route optimization across vehicles without exposing private driving data.
b. **Traffic management:** Federated models trained on distributed traffic sensor data can predict congestion, optimize signal timings, and improve urban mobility.
c. **Public safety:** Distributed learning on surveillance data enhances threat detection systems while maintaining citizens' privacy.

Projects like FedDrive and FL-based vehicular networks have demonstrated the scalability and efficiency of FL for real-time decision-making in connected transport systems, supporting the vision of intelligent, privacy-conscious smart cities.

5.5 Industrial and Manufacturing Networks

The Industry 4.0 revolution emphasizes interconnected manufacturing systems, where smart factories utilize IoT devices, sensors, and robots for automation and predictive maintenance [42]. However, industrial data often contain proprietary or sensitive operational information that cannot be shared externally.

Federated Learning enables collaborative optimization across multiple manufacturing sites without centralizing data. For example:

a. Predictive maintenance models can be trained across plants to detect machinery faults and optimize production schedules.
b. Quality control systems can learn from distributed sensor data to improve defect detection rates.
c. Supply chain optimization can leverage FL to enhance forecasting accuracy and resource distribution across partners.

In addition, energy-efficient and privacy-preserving FL frameworks in industrial settings support secure data collaboration while ensuring confidentiality of proprietary production data, enhancing resilience and operational efficiency.

Federated Learning has emerged as a versatile and scalable framework applicable across diverse distributed environments, from healthcare and finance to IoT and manufacturing [43]. Its core advantage lies in balancing intelligence and privacy, enabling collaborative innovation without data exposure. The continued adoption of FL across these domains underscores its transformative potential in building secure, efficient, and privacy-preserving AI ecosystems for the connected world

6 Comparative Analysis of Key Federated Learning Techniques

Over the years, several federated learning (FL) algorithms and privacy-preserving techniques have emerged to address challenges such as non-IID data, communication bottlenecks, and data confidentiality. This section presents a comparative summary of prominent FL algorithms (e.g., FedAvg, FedProx, FedMA) and privacy mechanisms (e.g., Differential Privacy, Homomorphic Encryption, Secure Multi-Party Computation), emphasizing their core principles, advantages, limitations, and suitable application areas.

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Caleb et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

6.1 Comparison of Federated Learning Algorithms

Algorithm	**Key Principle / Approach**	**Advantages**	**Limitations**	**Suitable Application Areas**
FedAvg (Federated Averaging)	Clients perform multiple local SGD steps; server aggregates weighted model updates.	Simple, efficient, and scalable; reduces communication frequency.	Performance degrades under highly non-IID data; potential fairness issues.	Mobile and edge computing, IoT devices, image classification.
FedProx (Federated Proximal)	Introduces a proximal term to the loss function to stabilize updates from heterogeneous data.	Handles client heterogeneity effectively; improves convergence stability.	Adds computation overhead; hyperparameter tuning is required.	Cross-device FL, healthcare, financial analytics.
FedMA (Federated Matched Averaging)	Matches and averages neurons between client models layer-by-layer instead of weight averaging.	Enhances model personalization; performs well with heterogeneous architectures.	Computationally complex; not ideal for large-scale networks.	Personalized healthcare, collaborative robotics, NLP.
FedNova (Federated Normalized Averaging)	Normalizes client updates to correct objective inconsistency in non-IID settings.	Faster convergence; improves model consistency across clients.	Sensitive to hyperparameter settings.	IoT analytics, mobile crowd sensing.
FedDyn (Federated Dynamic Regularization)	Introduces dynamic regularization to align local and global objectives.	Enhances convergence under data heterogeneity; robust to partial participation.	Requires additional computation for dynamic updates.	Cross-silo FL, smart city applications.
FedOpt (Federated Optimization Framework)	Employs adaptive optimization (e.g., Adam, Yogi) at the server side for global model aggregation.	Improves convergence rate and accuracy; adaptive to diverse client updates.	Higher computation at server; complex to tune.	Large-scale FL systems, financial prediction.
FedPer (Federated Personalization)	Separates model into shared and personalized layers for client-specific adaptation.	Improves local model accuracy and personalization.	Potential loss of generalization across clients.	Personalized mobile AI, recommender systems.

6.2 Comparison of Privacy-Preserving Mechanisms in FL

Privacy Method	Core Principle	Advantages	Limitations	Suitable Application Areas
Differential Privacy (DP)	Adds controlled random noise to gradients or parameters to obscure individual data contributions.	Formal privacy guarantees; easy to integrate with FL pipelines.	May reduce model accuracy due to noise; requires parameter tuning.	Healthcare, finance, user behavior modeling.

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Caleb et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

Homomorphic Encryption (HE)	Allows computation on encrypted data, ensuring confidentiality throughout aggregation.	Strong cryptographic protection; prevents data exposure during computation.	High computational cost; unsuitable for real-time or large-scale systems.	Secure data collaboration across institutions.
Secure Multi-Party Computation (SMPC)	Splits data or parameters into secret shares; computation is done collaboratively without revealing private values.	Prevents single-point data leakage; mathematically verifiable security.	High communication and computational overhead.	Cross-organizational learning, governmental data sharing.
Blockchain-Enabled FL	Integrates blockchain to ensure decentralized trust, auditability, and immutable record of model updates.	Transparency, traceability, and tamper-proof aggregation.	Scalability and latency issues; complex implementation.	Decentralized IoT systems, smart cities, supply chains.
Hybrid Approaches (DP + HE / DP + Blockchain)	Combines multiple privacy techniques to enhance protection and reduce weaknesses of individual methods.	Robust multi-layered privacy defense.	Complexity in coordination, increased computational load.	Critical infrastructures, finance, and defense networks.

6.3 Discussion

The comparative analysis reveals that no single FL algorithm or privacy technique universally outperforms others across all scenarios. The optimal choice depends on the application context, data characteristics, and system constraints:

a. FedAvg remains the baseline for most applications due to its simplicity and adaptability.
b. FedProx and FedDyn excel in heterogeneous environments by addressing data inconsistency and variable client performance.
c. FedMA and FedPer advance personalization, making them suitable for user-centric AI systems.
d. On the privacy front, Differential Privacy provides lightweight yet effective protection, while Homomorphic Encryption and SMPC ensure strong cryptographic security at higher computational cost.
e. Blockchain-based frameworks are emerging as promising solutions for achieving decentralized trust in multi-stakeholder collaborations.

In practical deployments, hybrid architectures, combining algorithmic optimization with privacy-enhancing technologies, are increasingly adopted to achieve a balance between model accuracy, efficiency, and data protection.

7 Conclusion

Federated Learning (FL) has emerged as a transformative paradigm in the evolution of privacy-preserving artificial intelligence, offering an effective solution to the growing tension between AI model performance and data confidentiality. By decentralizing the training process and allowing data to remain on local devices or institutional servers, FL enables collaborative model development without direct access to sensitive information. This approach not only mitigates privacy and security risks associated with centralized data storage but also aligns with modern data protection regulations such as GDPR and HIPAA.

Throughout this review, we have explored the conceptual foundations, architectural variants, and privacy-enhancing mechanisms of federated learning, including Differential Privacy (DP), Homomorphic Encryption (HE), Secure Multi-Party Computation (SMPC), and Blockchain-based frameworks. We also examined various optimization strategies, such as model compression, asynchronous coordination, and energy-efficient scheduling, that enhance scalability and

efficiency across distributed environments. Furthermore, we discussed how FL is revolutionizing key domains including IoT, healthcare, finance, smart cities, and industrial systems, where privacy and data sensitivity are paramount.

Despite these achievements, FL still faces persistent challenges such as data heterogeneity, communication overhead, security vulnerabilities, and lack of standardized evaluation frameworks. Addressing these limitations requires interdisciplinary innovation, combining advances in distributed computing, cryptography, and machine learning optimization.

Looking forward, the next generation of federated learning systems will likely evolve toward:

a. Hierarchical and cross-silo FL architectures for large-scale, multi-tier networks.
b. Personalized and adaptive FL to improve model relevance in heterogeneous settings.
c. Green and energy-efficient FL for sustainable deployment on edge and IoT devices.
d. Quantum-resistant and hybrid privacy frameworks that ensure long-term data protection.
e. Standardized benchmarks and reproducibility protocols to foster transparency and trust.

In essence, Federated Learning represents a critical step toward ethical, secure, and inclusive AI ecosystems. By bridging the gap between high-performance machine learning and stringent data privacy requirements, FL lays the foundation for a future where intelligent systems can learn collaboratively while respecting individual and institutional data sovereignty.

References

[1] A. J. Samuel, "AI and machine learning for secure data exchange in decentralized energy markets on the cloud," 2022.

[2] M. C. Myers, "Data Privacy Laws in the United States and Germany: Implications for Genomics Research and Personalized Medicine." University of Pittsburgh, 2024.

[3] B. Farahani and A. K. Monsefi, "Smart and collaborative industrial IoT: A federated learning and data space approach," *Digit. Commun. Networks*, vol. 9, no. 2, pp. 436–447, 2023.

[4] A. Yazdinejad, A. Dehghantanha, H. Karimipour, G. Srivastava, and R. M. Parizi, "A robust privacy-preserving federated learning model against model poisoning attacks," *IEEE Trans. Inf. Forensics Secur.*, vol. 19, pp. 6693–6708, 2024.

[5] C. Zhang, Y. Xie, H. Bai, B. Yu, W. Li, and Y. Gao, "A survey on federated learning," *Knowledge-Based Syst.*, vol. 216, p. 106775, 2021.

[6] N. Khan, S. Nisar, M. A. Khan, Y. A. U. Rehman, F. Noor, and G. Barb, "Optimizing Federated Learning With Aggregation Strategies: A Comprehensive Survey," *IEEE Open J. Comput. Soc.*, 2025.

[7] L. Collins, H. Hassani, A. Mokhtari, and S. Shakkottai, "Fedavg with fine tuning: Local updates lead to representation learning," *Adv. Neural Inf. Process. Syst.*, vol. 35, pp. 10572–10586, 2022.

[8] Z. Li, T. Lin, X. Shang, and C. Wu, "Revisiting weighted aggregation in federated learning with neural networks," in *International Conference on Machine Learning*, PMLR, 2023, pp. 19767–19788.

[9] Y. Liu *et al.*, "Vertical federated learning: Concepts, advances, and challenges," *IEEE Trans. Knowl. Data Eng.*, vol. 36, no. 7, pp. 3615–3634, 2024.

[10] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. V. Poor, "Federated learning for internet of things: A comprehensive survey," *IEEE Commun. Surv. Tutorials*, vol. 23, no. 3, pp. 1622–1658, 2021.

[11] J. Wen, Z. Zhang, Y. Lan, Z. Cui, J. Cai, and W. Zhang, "A survey on federated learning: challenges and applications," *Int. J. Mach. Learn. Cybern.*, vol. 14, no. 2, pp. 513–535, 2023.

[12] Q. Qian, J. Luo, and Y. Qin, "Heterogeneous federated domain generalization network with common representation learning for cross-load machinery fault diagnosis," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 54, no. 9, pp. 5704–5716, 2024.

[13] E. T. M. Beltrán *et al.*, "Decentralized federated learning: Fundamentals, state of the art, frameworks, trends, and challenges," *IEEE Commun. Surv. Tutorials*, vol. 25, no. 4, pp. 2983–3013, 2023.

[14] X. Zhao, W. Zhang, X. Xiao, and B. Lim, "Exploiting explanations for model inversion attacks," in *Proceedings of the IEEE/CVF international conference on computer vision*, 2021, pp. 682–692.

[15] Y. Zhao and J. Chen, "A survey on differential privacy for unstructured data content," *ACM Comput. Surv.*, vol. 54, no. 10s, pp. 1–28, 2022.
[16] J. Ling, J. Zheng, and J. Chen, "Efficient federated learning privacy preservation method with heterogeneous differential privacy," *Comput. Secur.*, vol. 139, p. 103715, 2024.
[17] Z. Abou El Houda, "Cyber threat actors review: examining the tactics and motivations of adversaries in the cyber landscape," in *Cyber Security for Next-Generation Computing Technologies*, CRC Press, 2024, pp. 84–101.
[18] M. Bethany, A. Galiopoulos, E. Bethany, M. B. Karkevandi, N. Vishwamitra, and P. Najafirad, "Large language model lateral spear phishing: A comparative study in large-scale organizational settings," *arXiv Prepr. arXiv2401.09727*, 2024.
[19] M. Smeets, *Ransom War: How Cyber Crime Became a Threat to National Security*. Oxford University Press, 2025.
[20] F. N. Wirth, T. Meurers, M. Johns, and F. Prasser, "Privacy-preserving data sharing infrastructures for medical research: systematization and comparison," *BMC Med. Inform. Decis. Mak.*, vol. 21, no. 1, p. 242, 2021.
[21] D. Javeed, M. S. Saeed, P. Kumar, A. Jolfaei, S. Islam, and A. K. M. N. Islam, "Federated learning-based personalized recommendation systems: An overview on security and privacy challenges," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 2618–2627, 2023.
[22] P. O. Ufomba and O. S. Ndibe, "IoT and Network Security: Researching Network Intrusion and Security Challenges in Smart Devices," *Commun. Phys. Sci.*, vol. 9, no. 4, pp. 784–800, 2023.
[23] K. Munjal and R. Bhatia, "A systematic review of homomorphic encryption and its contributions in healthcare industry," *Complex Intell. Syst.*, vol. 9, no. 4, pp. 3759–3786, 2023.
[24] Z. Wang, "Confidential Federated Learning with Homomorphic Encryption." 2023.
[25] M. Ghorbanizad, "Privacy-Preserving Federated Learning Architecture for Secure Patient Data Sharing in Hospital Networks." Polytechnique Montréal, 2025.
[26] M. Rahaman, V. Arya, S. M. Orozco, and P. Pappachan, "Secure multi-party computation (SMPC) protocols and privacy," in *Innovations in Modern Cryptography*, IGI Global, 2024, pp. 190–214.
[27] M. M. Orabi, O. Emam, and H. Fahmy, "Adapting security and decentralized knowledge enhancement in federated learning using blockchain technology: literature review," *J. Big Data*, vol. 12, no. 1, p. 55, 2025.
[28] K. N. Mishra, R. K. Lal, P. N. Barwal, and A. Mishra, "Advancing Data Privacy in Cloud Storage: A Novel Multi-Layer Encoding Framework," *Appl. Sci.*, vol. 15, no. 13, p. 7485, 2025.
[29] P. V. Dantas, W. Sabino da Silva Jr, L. C. Cordeiro, and C. B. Carvalho, "A comprehensive review of model compression techniques in machine learning," *Appl. Intell.*, vol. 54, no. 22, pp. 11804–11844, 2024.
[30] J. Peng, Z. Li, S. Shi, and B. Li, "Sparse Gradient Communication with AlltoAll for Accelerating Distributed Deep Learning," in *Proceedings of the 53rd International Conference on Parallel Processing*, 2024, pp. 148–157.
[31] Z. Li *et al.*, "Data heterogeneity-robust federated learning via group client selection in industrial IoT," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17844–17857, 2022.
[32] J. Nguyen *et al.*, "Federated learning with buffered asynchronous aggregation," in *International conference on artificial intelligence and statistics*, PMLR, 2022, pp. 3581–3607.
[33] J. Liu *et al.*, "Adaptive asynchronous federated learning in resource-constrained edge computing," *IEEE Trans. Mob. Comput.*, vol. 22, no. 2, pp. 674–690, 2021.
[34] P. Mishra and G. Singh, "Energy management systems in sustainable smart cities based on the internet of energy: A technical review," *Energies*, vol. 16, no. 19, p. 6903, 2023.
[35] S. Zhan, L. Huang, G. Luo, S. Zheng, Z. Gao, and H.-C. Chao, "A Review on Federated Learning Architectures for Privacy-Preserving AI: Lightweight and Secure Cloud–Edge–End Collaboration," *Electronics*, vol. 14, no. 13, p. 2512, 2025.
[36] G. Paolone, D. Iachetti, R. Paesani, F. Pilotti, M. Marinelli, and P. Di Felice, "A holistic overview of the internet of things ecosystem," *IoT*, vol. 3, no. 4, pp. 398–434, 2022.
[37] I. A. Alnajjar, L. Almazaydeh, A. A. Odeh, A. A. Salameh, K. Alqarni, and A. A. Ban Atta, "Anomaly Detection Based on Hierarchical Federated Learning with Edge-Enabled Object Detection for Surveillance Systems in Industry 4.0 Scenario.," *Int. J. Intell. Eng. Syst.*, vol. 17, no. 4, 2024.
[38] F. H. Semantha, S. Azam, B. Shanmugam, K. C. Yeo, and A. R. Beeravolu, "A conceptual framework to ensure privacy in patient record management system," *IEEE Access*, vol. 9, pp. 165667–165689, 2021.
[39] E. Albalawi *et al.*, "Integrated approach of federated learning with transfer learning for classification and diagnosis of brain tumor," *BMC Med. Imaging*, vol. 24, no. 1, p. 110, 2024.

[40] A. Oluwaferanmi, "Cross-Border Data Sharing and AI in AML: Legal and Operational Implications," 2025.
[41] S. Kaleem, A. Sohail, M. U. Tariq, and M. Asim, "An improved big data analytics architecture using federated learning for IoT-enabled urban intelligent transportation systems," *Sustainability*, vol. 15, no. 21, p. 15333, 2023.
[42] S. Dabic-Miletic, "Advanced technologies in smart factories: A cornerstone of industry 4.0," *J. Ind. Intell.*, vol. 1, no. 3, pp. 148–157, 2023.
[43] K. Lazaros, D. E. Koumadorakis, A. G. Vrahatis, and S. Kotsiantis, "Federated learning: Navigating the landscape of collaborative intelligence," *Electronics*, vol. 13, no. 23, p. 4744, 2024.