1. INTRODUCTION

Artificial Intelligence (AI) has revolutionized numerous industries by enabling intelligent decision-making and automation. The success of AI largely depends on the availability of large, diverse datasets to train machine learning models. However, collecting and centralizing these datasets pose significant privacy concerns, as sensitive information may be exposed or misused. Furthermore, data-sharing regulations like GDPR and HIPAA restrict the transfer of personal and confidential data, creating challenges for collaborative AI development.

Federated Learning (FL) is a cutting-edge solution to these challenges, allowing multiple devices or organizations to jointly train machine learning models without sharing raw data. In FL, data remains on local devices, and only model updates—such as weights or gradients—are shared with a central server for aggregation. This decentralized approach protects user privacy, reduces the risk of data leaks, and ensures compliance with strict data protection laws. It also empowers organizations to collaborate and benefit from collectively trained models without compromising data ownership.

This report explores the essential aspects of federated learning, including its historical background, core algorithms like federated averaging and secure aggregation, system architectures, and applications in fields such as healthcare, finance, and mobile applications. It further discusses the benefits, challenges, and ongoing research efforts to make federated learning more efficient, secure, and scalable. The aim is to provide readers with a clear understanding of how federated learning is shaping the future of privacy-aware AI.

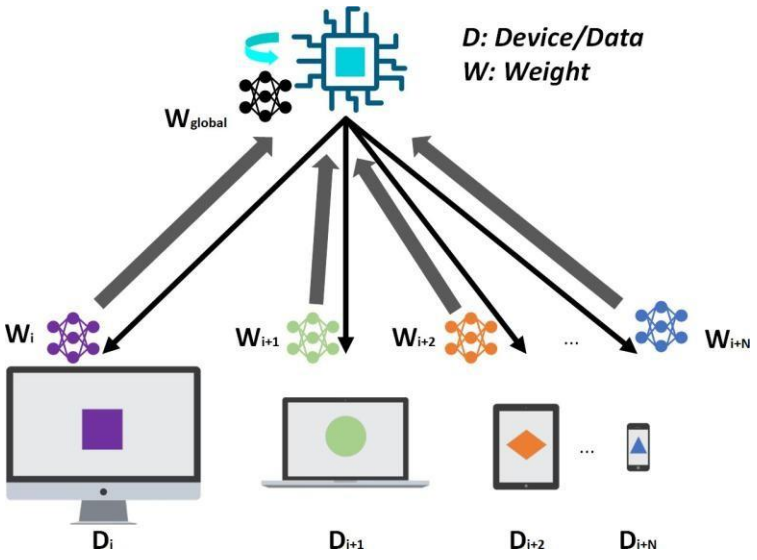


Figure: Federated learning concept.

2. HISTORY

Federated Learning (FL) originated from distributed machine learning research in the 1990s and 2000s that aimed to train models across decentralized devices without centralizing data, focusing on efficiency and fault tolerance. The modern FL paradigm was formally introduced by Google in 2016 with the Federated Averaging (FedAvg) algorithm, enabling privacy- preserving collaborative training across millions of devices by aggregating local model updates instead of raw data. Building on this foundation, academic and industry research advanced FL by integrating privacy-enhancing techniques like secure multiparty computation, differential privacy, and homomorphic encryption, while data regulations such as GDPR accelerated its adoption. Today, FL is widely applied in sensitive domains like healthcare, finance, and IoT, with ongoing efforts to improve communication efficiency, robustness, and scalability for secure, decentralized AI model training.

2a. Early Distributed Learning Concepts

The foundations of federated learning were laid in the late 20th century through research in distributed machine learning. Initially, the focus was on splitting large datasets across multiple computing nodes to speed up training and make it more fault tolerant. These early models distributed data and computation but required centralized access to data logs or lacked robust privacy guarantees. Although these methods inspired decentralized computing, the need to protect sensitive information was not explicitly addressed in these first attempts.

2b. Introduction of Federated Learning Paradigm

The formal concept of federated learning was introduced by Google researchers in 2016 with the Federated Averaging (FedAvg) algorithm. This innovation allowed model training on decentralized devices such as smartphones, where data remained on the device and only model updates were sent to a central server. This approach not only preserved user privacy but also reduced communication costs by transmitting smaller model updates instead of large datasets. Subsequently, the success of FedAvg spurred widespread research and development, resulting in various enhancements to improve efficiency, scalability, and robustness against adversarial attacks.

2c. Advances in Privacy-Preserving Techniques

Building on the foundational federated learning framework, researchers introduced various privacy-enhancing methods to strengthen data protection. Techniques such as secure multiparty computation allow multiple parties to compute functions collaboratively without revealing their inputs. Differential privacy adds calibrated noise to model updates to prevent tracing back to individual data points. Homomorphic encryption enables operations on encrypted data, ensuring that sensitive information remains protected even during processing. Integrating these methods within federated learning frameworks has significantly improved its security guarantees, making FL viable in privacy-critical domains like healthcare and finance, where data confidentiality is paramount.

2d. Current Trends and Industrial Adoption

Federated learning has rapidly transitioned from research to real-world applications across industries such as healthcare, finance, and mobile technology. Organizations use FL to enable collaborative model training while respecting data privacy laws and minimizing data exposure risks. Current research focuses on improving communication efficiency, enhancing security against adversarial attacks, and scaling federated learning to networks with millions of heterogeneous devices. Emerging applications in Internet of Things (IoT), personalized medicine, and edge computing highlight FL's potential to become the foundation for privacy- conscious AI in the digital age.

3. HOW FEDERATED LEARNING WORKS

3a. Overview of the architecture and process

Federated learning is a distributed machine learning technique where deep learning models are trained locally on edge devices holding private data. The central server initializes a global model and distributes it to clients, which perform local training on their data. Clients then send updated model weights to the server, which aggregates these updates—often using the federated averaging algorithm—to form an improved global model. This updated global model is redistributed to clients, and the process repeats until convergence. The architecture typically involves three key components: (a) the orchestrator that manages training rounds, (b) the aggregator that combines model updates securely, and (c) the client or worker that trains models locally. This approach enables collaborative learning without sharing sensitive raw data, addressing privacy and regulatory concerns.

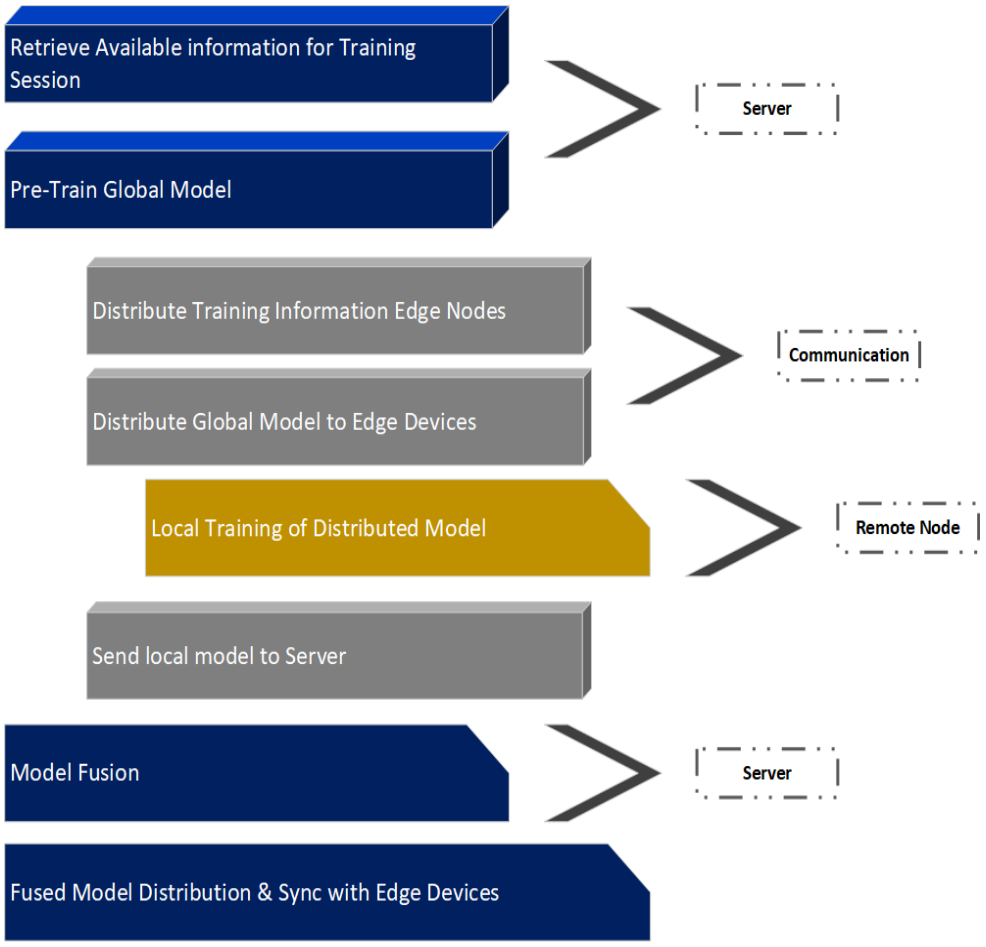


Figure: Simple federated learning pipeline.

3b. Orchestrator

The orchestrator is responsible for managing the federated learning process, including initiating the FL session, selecting the population of devices, organizing the data, algorithm, and pipeline, setting the training context, managing communication and security, evaluating the performance, and, finally, synchronizing the FL procedure.

3c. Aggregator

The aggregator is responsible for incorporating the updates from the local models into the global model. In some cases, the orchestrator also acts as the aggregator, particularly for smaller networks or certain security or operational requirements. The aggregator also implements security and privacy measures to protect the FL server and workers from any malicious actors.

3d. Worker

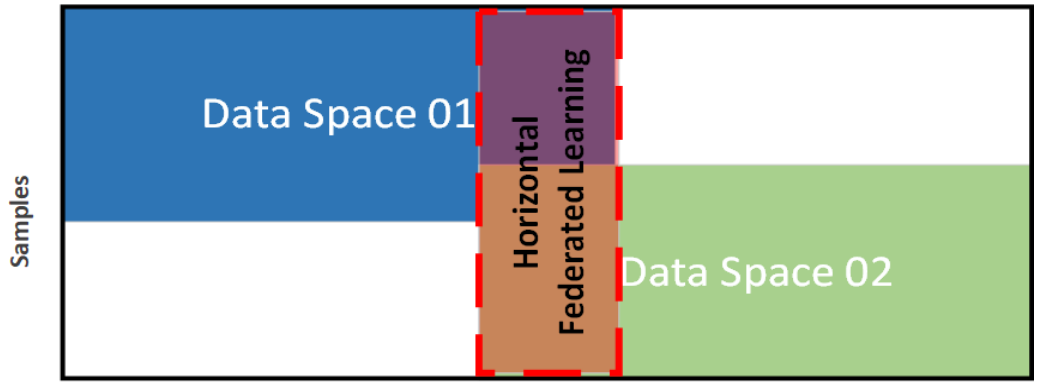
The worker, also known as the party, is responsible for the local training that takes place during the FL training session. The worker is the owner of the data and updates its model based on the newly received version of the global model after the local training and global model generation by the aggregator. The worker has the option of participating in the FL session or not, depending on resource allocation or criticality.

The above mentioned components established the foundation of the methodology. Depending on the type and nature of the deployment, these components can have additional responsibilities and placement or some extra components might be added. The different types of FL are described in the next section.

4. TYPES OF FEDERATED LEARNING

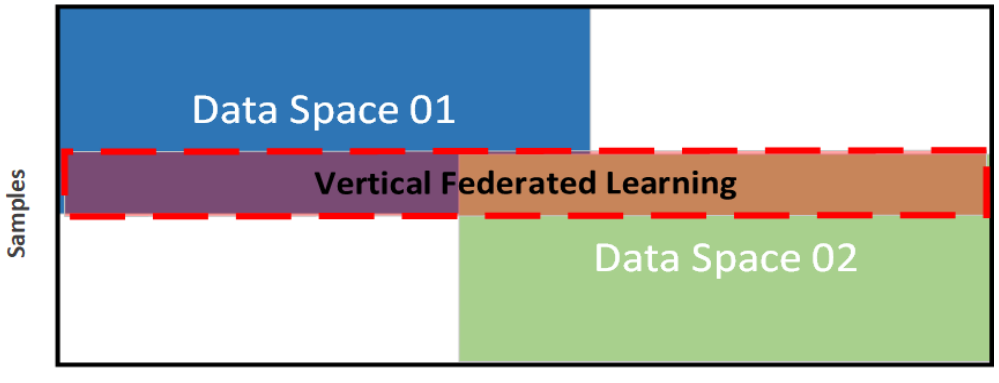
There is a variety of different federated learning application types that depend on a multitude of characteristics. A main characteristic that defines the type of the methodology applied is the way that data and their features are distributed and used by the different nodes. In particular, based on the data, we have the following:

- **Horizontal federated learning:** This type of approach trains models on data that is horizontally partitioned across different devices or entities. For example, training a model on data from different hospitals or different companies (Figure 5.1).



Horizontal Federated Learning

- **Vertical federated learning:** This type of federated learning trains models on data that is vertically partitioned across different devices or entities. For example, training a model on data from different features of the same patient (Figure 5.2).



Vertical Federated Learning

Table: Common fusion algorithms used in FL.

Algorithm	Year	Description	Benefits
FedAvg	2017	An iterative model averaging FL framework	Reduces communication cost by locally computed updated aggregation
Zoo	2018	Composable services to deploy ML models locally on edge	Reduces latency in data processing, and minimizes the raw data revealed.
FedPer	2019	Federated learning with personalization layers	Improves results with data heterogeneity, and communication Cost.
FedAsync	2019	Asynchronous federated optimization framework	Improves flexibility and Scalability and tolerates staleness
FedCS	2019	Client selection for FL with heterogeneous resources	Improves performance and reduces training time
BlockFL	2019	Block chained federated architecture	Optimizes communication, computation, and latency
FedMa	2020	Federated matched aver-aging algorithm for FL	Improves accuracy and communication cost
FedAT	2020	Synchronous intra-tier training and asynchronous cross-tier training	Improves accuracy and reduces communication cost

11. ADVANTAGES AND DISADVANTAGES

By itself and1 as it is probably apparent, the federated learning approach is vast and, in its range, it encapsulates major advantages but also some drawbacks. As in all fields, the optimal deployment of federated learning is the fine line between the tradeoff of these advantages and drawback and strictly depends on the application of the methodology. For example, there might be some applications that require better model generalization but in expense of the communication efficiency of the network. Table 12.1 enumerates some of these advantages and disadvantages of federated learning in order to provide a better view of its utility.

Table: Advantages and disadvantages of federated learning.

Advantages	Disadvantages
Collaborative learning: Allows multiple devices or entities to collaboratively train a model while keeping their data on-device. This allows for the training of models on large amounts of data without the need to transmit or centralize	**Data availability**: Data availability can be an issue in federated learning, as not all devices or entities may have access to the same data or may have data of different quality.
Data privacy and security: Allows for the training of models without com- promising the privacy and security of the data. This is particularly important in scenarios where data is sensitive or distributed across multiple devices.	**Communication overhead:** Requires communication between the devices or entities, which can be a bottleneck, especially if the devices are located in different geographical locations.
Edge computing: Allows devices to train models locally, which can reduce the need for transmitting large amounts of data over the network. Additionally, it enables the training of models that can be deployed on resource- constrained devices, such as IoT sensors or mobile phones.	**Model divergence:** Can suffer from model divergence, where the local models may not con- verge to a common global model due to the non-IID data distribution on the devices.
Handling non-IID data: It is particularly well-suited for training models on non-IID data that is commonly found in the real-world scenarios.	**Latency:** Can suffer from latency issues, as it requires communication between the devices or entities to exchange model updates.
Scalability: It is highly scalable and can handle a large number of devices or entities.	**Complexity:** Can be complex to implement and requires a lot of communication and coordination between the devices or entities.

12. APPLICATIONS OF FEDERATED LEARNING

Here is more detailed information on the applications of federated learning:

1. **Healthcare:**

Federated learning enables hospitals and research institutes to train AI models on patient data across multiple locations without sharing raw health records. This approach supports disease prediction, personalized treatment plans, and medical image analysis while preserving patient privacy. For example, FL has been used for improving diagnostic models for illnesses like cancer and COVID-19 by aggregating insights from diverse clinical datasets.

2. **Finance:**

Banks, insurers, and financial firms adopt federated learning for fraud detection, risk assessment, and anti-money laundering. FL allows these institutions to collaborate on training models using combined customer data without exposing proprietary or personal information. This helps improve detection capabilities and regulatory compliance simultaneously.

3. **Mobile and Edge Devices:**

Tech companies use FL for on-device personalization features such as keyboard suggestions, voice recognition, and recommendation engines. The local training on phones or smart devices prevents sensitive personal data from being uploaded to servers while refining AI models continuously from diverse user environments.

4. **Smart Cities and IoT:**

Federated learning support data-driven smart city applications like traffic monitoring, smart metering, and public safety by aggregating data from dispersed sensors and connected devices without data centralization. This enhances real-time intelligence and decision-making while respecting privacy norms.

5. **Retail and Marketing:**

Retailers employ FL to improve customer segmentation, product recommendations, and inventory management by combining insights from online and offline sales data across stores. Federated approaches ensure customer privacy and data compliance.