FEDERATED LEARNING

A SEMINAR REPORT

Submitted in partial fulfilment for the award of the Degree of

BACHELOR OF TECHNOLOGY

(Computer Science Engineering)

SUBMITTED BY

NAME OF STUDENT	**ENROLL**
MURSALEEN MOHI-UD-DIN	**190333**

Department of Computer Science Engineering

Government College of Engineering & Technology

Safapora, Ganderbal -193504, J&K(India)

September, 2023

Government College of Engineering & Technology

Safapora, Ganderbal –193504, J&K (India)

CERTIFICATE

This is to certify that the project titled "**Federated Learning"** is a bonafide record of the work done under my supervision & guidance by **MURSALEEN MOHI-UD-DIN (190333),** in partial fulfilment of the requirements for the award of the degree of Bachelors of Technology in Electrical & Electronics Engineering of GOVERNMENT COLLEGE OF ENGINEERING AND TECHNOLOGY-SAFAPORA GANDERBAL, during the year 2023.

Dr. Nisar Iqbal Wani
(Head Of Department)
(Department of CSE)

Ms. Bisma Rasheed
(Assistant Professor)
(Department of CSE)

CANDIDATES' DECLARATION

We hereby certify that the project titled **"Federated Learning**" submitted to the Department of Computer Science Engineering of GOVERNMENT COLLEGE OF ENGINEERING AND TECHNOLOGY-SAFAPORA GANDERBAL, is an authentic record of our work carried out during the period of August 2023 to September 2023 under the guidance of Ms. Bisma Rasheed.

The matter presented in this major project report has not been submitted by us to any other Institute/ University for the award of any Degree/ Diploma.

MURSALEEN MOHI-UD-DIN 190333

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

Signature of the Assistant Professor.

ACKNOWLEDGEMENT

As a matter of first importance, we thank to almighty Allah for all the blessings in the entirety of our undertakings.

We take this opportunity to express our profound gratitude and deep regards to our Principal *Prof. (Dr.) Rauf Ahmad Khan,* for his exemplary guidance, monitoring and constant encouragement throughout the course of engineering.

We also take this opportunity to express a deep sense of gratitude to *Dr. Nisar Iqbal Wani,* Assistant Professor & Head (Department of Computer Science Engineering), for his cordial support, valuable information & guidance, which helped us in completing this task through various stages. His guidance shall carry is in long way in the journey of life which we are about to embark.

We are obliged to *Ms. Bisma Rasheed,* Assistant Professor (Department of Computer Science Engineering), for the valuable information and technical help and guidance from time to time in completion of this project.

Lastly, we thank our parents, family & friends for their constant encouragement and support.

Place: GCET SAFAPORA MURSALEEN MOHI-UD-DIN

Date:

ABSTRACT

Federated learning involves training statistical models over remote devices or siloed data centers, such as mobile phones or hospitals, while keeping data localized. Training in heterogeneous and potentially massive networks introduces novel challenges that require a fundamental departure from standard approaches for large-scale machine learning, distributed optimization, and privacy-preserving data analysis. In this article, we discuss the unique characteristics and challenges of federated learning, provide a broad overview of current approaches, and outline several directions of future work that are relevant to a wide range of research. Federated learning (FL) has been developed as a promising framework to leverage the resources of edge devices, enhance customers' privacy, comply with regulations, and reduce development costs. Although many methods and applications have been developed for FL, several critical challenges for practical FL systems remain unaddressed. Federated learning, a cutting-edge method of distributed learning, enables multiple users to share training results while maintaining the privacy of their personal data. Collecting data from different data owners for making machine learning predictions becomes increasingly challenging as data security becomes more of a priority. Federated learning protects user's privacy in addition to increase the training data while overcoming the challenges faced by machine learning and deep learning models. Since the data privacy and security is a world-wide concern, the concept of federated learning is increasing day by day from theoretical to practical level.

List of Tables

LIST OF FIGURES

NOMENCLATURE

English Symbols

FLC	Federated Learning Client
FLS	Federated Learning Server
IID	Independent and Identically Distributed
DNN	Deep Neural Network
DP	Differential Privacy
SGD	Stochastic Gradient Descent
CNN	Convolutional Neural Network
RNN	Recurrent Neural Network
LSTM	Long Short-Term Memory
P2P	Peer-to-Peer
MLP	Multilayer Perceptron

ABBREVIATIONS

FL	Federated Learning
AI	Artificial intelligence
IoT	Internet of Things
ML	Machine Learning
CPU	Central Processing Unit
GPU	Graphics Processing Unit
API	Application Programming Interface
GDPR	General Data Protection Regulation

CONTENTS

CHAPTER 3 FEDERATED LEARNING FUNDAMENTALS

CHAPTER 4 COMPARING FEDERATED LEARNING TO OTHER TYPES OF LEARNING

CHAPTER 5 MAIN FEATURES

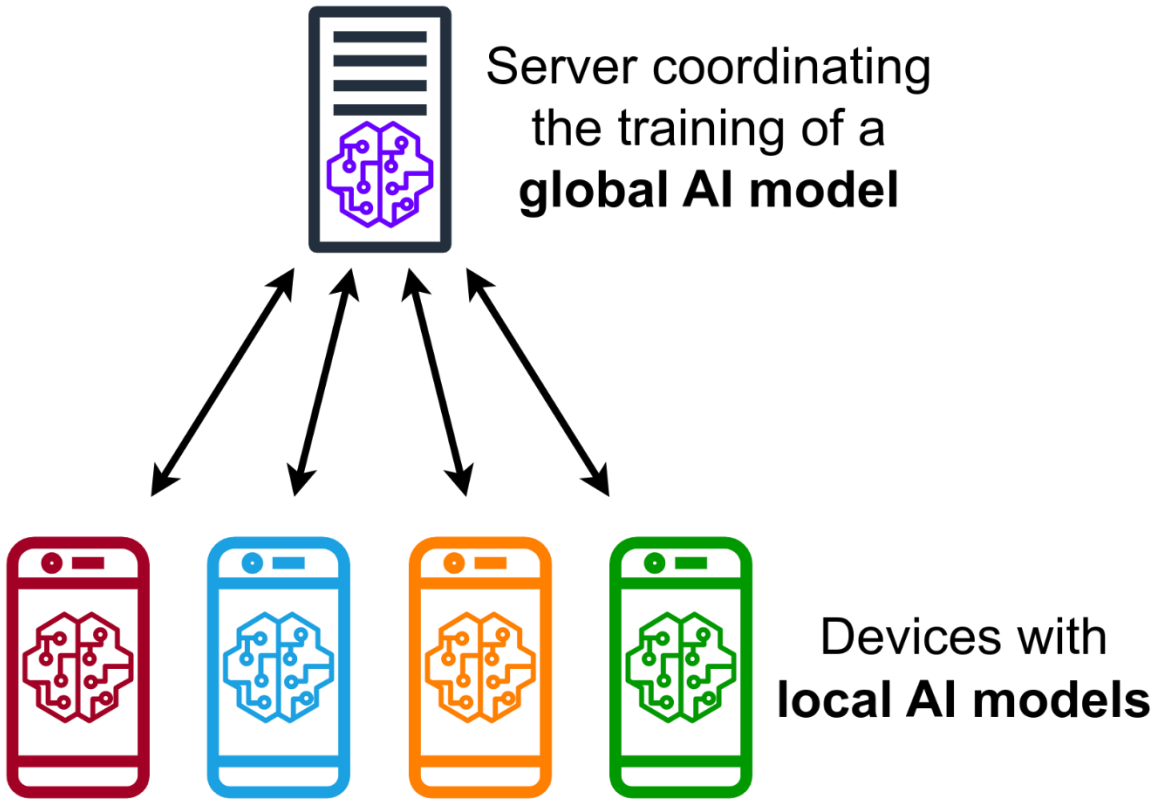
CHAPTER 6 FEDERATED LEARNING VARIATIONS

CHAPTER 7 FEDERATED LEARNING USE CASES

INTRODUCTION

Federated learning (also known as collaborative learning) is a machine learning technique that trains an algorithm via multiple independent sessions, each using its own dataset. This approach stands in contrast to traditional centralized machine learning techniques where local datasets are merged into one training session, as well as to approaches that assume that local data samples are identically distributed.

Federated learning enables multiple actors to build a common, robust machine learning model without sharing data, thus addressing critical issues such as data privacy, data security, data access rights and access to heterogeneous data. Its applications engage industries including defense, telecommunications, Internet of Things, and pharmaceuticals. A major open question is when/whether federated learning is preferable to pooled data learning. Another open question concerns the trustworthiness of the devices and the impact of malicious actors on the learned model.



1.1 DEFINITION

Federated learning aims at training a machine learning algorithm, for instance deep neural networks, on multiple local datasets contained in local nodes without explicitly exchanging data samples. The general principle consists in training local models on local data samples and exchanging parameters (e.g., the weights and biases of a deep neural network) between these local nodes at some frequency to generate a global model shared by all nodes.

The main difference between federated learning and distributed learning lies in the assumptions made on the properties of the local datasets, as distributed learning originally aims at parallelizing computing power where federated learning originally aims at training on heterogeneous datasets. While distributed learning also aims at training a single model on multiple servers, a common underlying assumption is that the local datasets are independent and identically distributed and roughly have the same size. None of these hypotheses are made for federated learning; instead, the datasets are typically heterogeneous and their sizes may span several orders of magnitude. Moreover, the clients involved in federated learning may be unreliable as they are subject to more failures or drop out since they commonly rely on less powerful communication media (i.e. Wi-Fi) and battery-powered systems (i.e. smartphones and IoT devices) compared to distributed learning where nodes are typically datacenters that have powerful computational capabilities and are connected to one another with fast networks.

1.2 CENTRALIZED FEDERATED LEARNING

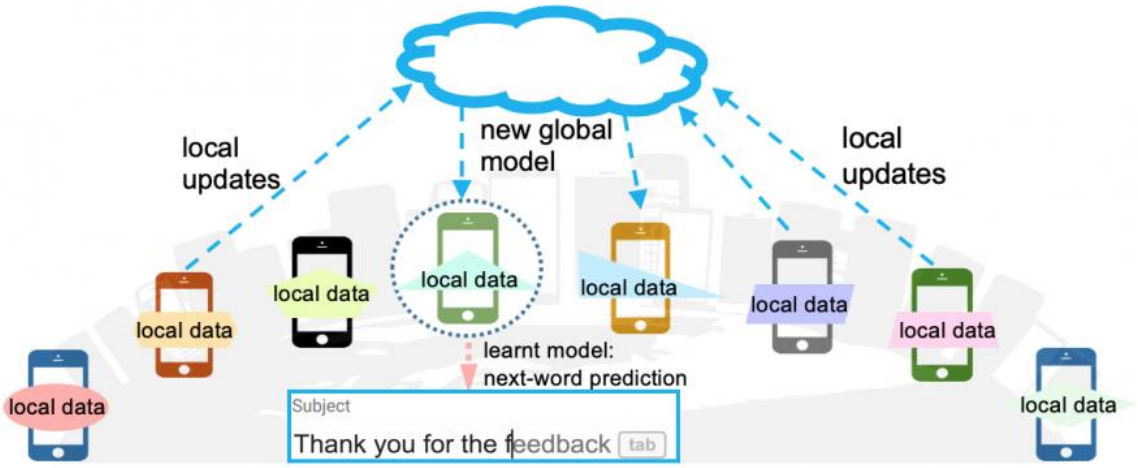
In the centralized federated learning setting, a central server is used to orchestrate the different steps of the algorithms and coordinate all the participating nodes during the learning process. The server is responsible for the node's selection at the beginning of the training process and for the aggregation of the received model updates. Since all the selected nodes have to send updates to a single entity, the server may become a bottleneck of the system.

1.3 DECENTRALIZED FEDERATED LEARNING

In the decentralized federated learning setting, the nodes are able to coordinate themselves to obtain the global model. This setup prevents single point failures as the model updates are exchanged only between interconnected nodes without the orchestration of the central server. Nevertheless, the specific network topology may affect the performances of the learning process. See blockchain-based federated learning and the references therein.

1.4 HETEROGENOUS FEDERATED LEARNING

An increasing number of application domains involve a large set of heterogeneous clients, e.g., mobile phones and IoT devices. Most of the existing Federated learning strategies assume that local models share the same global model architecture. Recently, a new federated learning framework named HeteroFL was developed to address heterogeneous clients equipped with very different computation and communication capabilities. The HeteroFL technique can enable the training of heterogeneous local models with dynamically varying computation and non-iid data complexities while still producing a single accurate global inference model.



Devices communicate with a central server periodically to learn a global model. Federated learning helps preserve user privacy and reduce strain on the network by keeping data localized.

CHAPTER 2

LITERATURE SURVEY

2.1 INTRODUCTION

The literature survey chapter serves as a foundation for understanding Federated Learning by examining existing research and developments in the field. It provides insights into the historical evolution of Federated Learning and reviews significant contributions made by researchers and organizations. This chapter is divided into several sections to explore the key aspects of Federated Learning through the lens of prior research.

2.2 EVOLUTION OF FEDERATED LEARNING

This section traces the evolution of Federated Learning from its conceptual beginnings to its current state. It discusses seminal papers, projects, and milestones in the development of FL, emphasizing how it has evolved in response to the changing landscape of data privacy and distributed computing.

2.3 FEDERATED LEARNING ALGORITHMS

In this section, we delve into the core algorithms that drive Federated Learning. It provides an overview of various algorithms used in FL, including Federated Averaging, Federated Stochastic Gradient Descent (SGD), and other federated optimization techniques. We will explore their advantages, limitations, and real-world applications.

2.4 FEDERATED LEARNING APPLICATIONS

This section highlights the diverse applications of Federated Learning across industries. We discuss case studies and use cases where FL has been successfully implemented, including healthcare, finance, edge computing, and Internet of Things (IoT). Real-world examples demonstrate how FL addresses data privacy concerns while delivering meaningful results.

2.5 FEDERATED LEARNING CHALLENGES

An important aspect of Federated Learning is understanding its challenges and limitations. This section delves into the technical and practical challenges associated with FL, such as communication overhead, non-IID data distribution, and security concerns. It also discusses privacy-preserving mechanisms like Differential Privacy (DP) and Secure Multi-Party Computation (SMPC) in the context of FL.

2.6 FEDERATED LEARNING IN RESEARCH AND INDUSTRY

This section explores how Federated Learning has been adopted in both academic research and industry. It provides insights into ongoing research efforts and projects by tech giants like Google, Apple, and Microsoft. We discuss open-source FL frameworks, tools, and libraries that facilitate experimentation and adoption.

2.7 SUMMARY OF LITERATURE

The literature survey chapter concludes with a summary of the key takeaways from the reviewed literature. It synthesizes the findings, identifies trends, and lays the groundwork for the subsequent chapters, where we will delve deeper into the technical aspects, challenges, and applications of Federated Learning.
By the end of this chapter, readers will have gained a comprehensive understanding of the historical context, core algorithms, applications, and challenges of Federated Learning, providing a solid foundation for the more detailed discussions that follow.

CHAPTER 3

FEDERATED LEARNING FUNDAMENTALS

3.1 INTRODUCTION

Chapter 3 delves into the fundamental principles of Federated Learning (FL). Building on the insights gained from the literature survey, this chapter aims to provide a deeper understanding of the core concepts that underpin FL. It explores the basic workflow, components, and essential techniques involved in Federated Learning.

3.2 FEDERATED LEARNING WORKFLOW

This section begins by describing the high-level workflow of Federated Learning. It illustrates how FL enables model training across distributed devices while preserving data privacy. The key components, including Federated Learning Clients (FLCs), Federated Learning Servers (FLS), and model updates, are introduced, shedding light on the orchestration of FL.

3.3 FEDERATED LEARNING MODELS

In this subsection, we explore the types of models commonly used in Federated Learning, including Deep Neural Networks (DNNs), Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Long Short-Term Memory (LSTM) networks. Understanding these models is crucial for comprehending how FL adapts them to distributed and privacy-preserving settings.

3.4 DATA PRIVACY IN FEDERATED LEARNING

Data privacy is a cornerstone of FL. This subsection focuses on the mechanisms and technologies that safeguard privacy during the Federated Learning process. Topics covered include Differential Privacy (DP), Secure Multi-Party Computation (SMPC), and federated learning with homomorphic encryption.

3.5 MODEL AGGREGATION AND EVALUATION

Model aggregation is a critical step in FL where updates from multiple clients are combined to create a global model. This section explains aggregation methods, such as weighted averaging and secure aggregation, and highlights the importance of model evaluation and validation in federated settings.

3.6 FEDERATED LEARNING FRAMEWORKS AND TOOLS

An overview of popular Federated Learning frameworks and tools is presented in this subsection. It discusses open-source libraries like TensorFlow Federated and PySyft, which facilitate the implementation of FL in research and industry.

3.8 CURRENT RESEARCH TOPICS

Federated learning has started to emerge as an important research topic in 2015 and 2016, with the first publications on federated averaging in telecommunication settings. Another important aspect of active research is the reduction of the communication burden during the federated learning process. In 2017 and 2018, publications have emphasized the development of resource allocation strategies, especially to reduce communication requirements between nodes with gossip algorithms as well as on the characterization of the robustness to differential privacy attacks. Other research activities focus on the reduction of the bandwidth during training through sparsification and quantization methods, where the machine learning models are sparsified and/or compressed before they are shared with other nodes. Developing ultra-light DNN architectures is essential for device-/edge- learning and recent work recognizes both the energy efficiency requirements for future federated learning and the need to compress deep learning, especially during learning.

Recent research advancements are starting to consider real-world propagating channels as in previous implementations ideal channels were assumed. Another active direction of research is to develop Federated learning for training heterogeneous local models with varying computation complexities and producing a single powerful global inference model.

A learning framework named Assisted learning was recently developed to improve each agent's learning capabilities without transmitting private data, models, and even learning objectives. Compared with Federated learning that often requires a central controller to orchestrate the learning and optimization, assisted learning aims to provide protocols for the agents to optimize and learn among themselves without a global model.

3.9 SUMMARY OF FUNDAMENTALS

Chapter 3 concludes with a summary that distills the fundamental concepts of Federated Learning. Readers will leave this chapter with a comprehensive understanding of the workflow, models, algorithms, privacy mechanisms, and evaluation methods that constitute the foundation of FL.

By mastering these fundamental principles, readers will be well-equipped to explore the advanced topics and applications discussed in the subsequent chapters.

CHAPTER 4

COMPARING FEDERATED LEARNING TO OTHER TYPES OF LEARNING

4.1 COMPARISON

There are lots of potential learning processes in machine learning. As we saw, federated learning is a decentralized approach that maintains data private on devices and allows for flexible datasets.

However, we can also cite centralized learning, which stores data on a server resulting in low privacy and fixed datasets; distributed learning as another decentralized approach with moderate privacy and bandwidth requirements limited by fixed nodes and active learning, which selects informative data points for labeling with low privacy and limited flexibility due to fixed dataset usage.

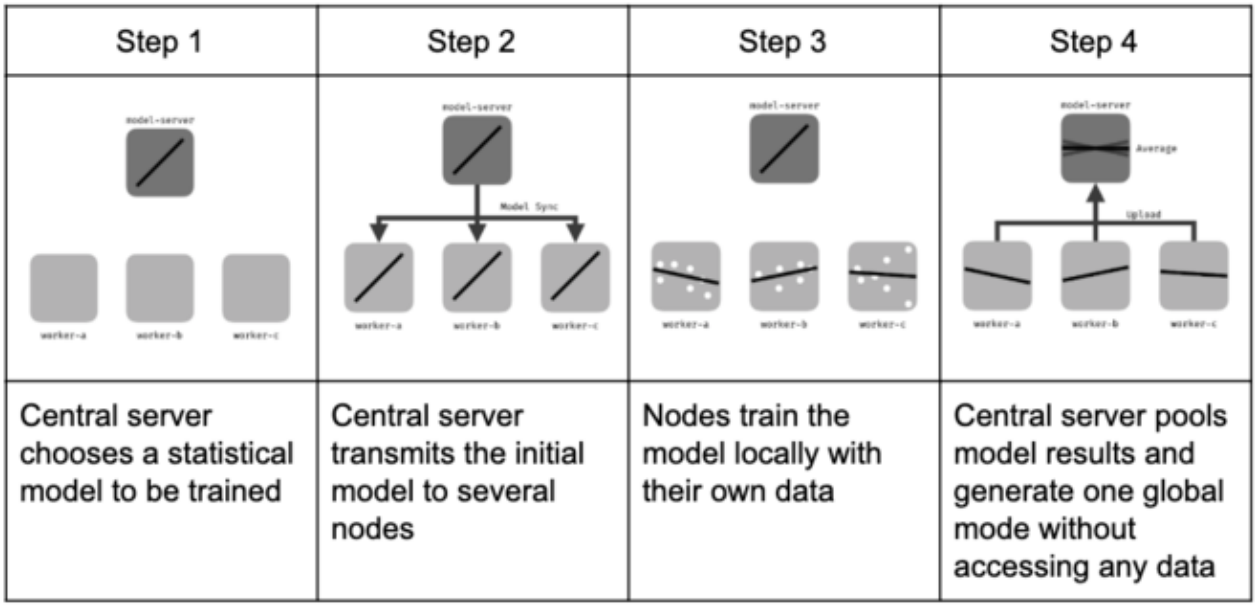
Learning Type	Data Centralization	Privacy	Bandwidth Requirements	Model Flexibility
Federated Learning	Decentralized, data remains on devices	High privacy, data not sent to central server	Low, only trained models sent back to server	Dynamic dataset allows for improved flexibility
Centralized Learning	Data is centralized on a server	Low privacy, data stored on server	High, raw data sent to server for analysis	Limited by fixed dataset, less flexible
Distributed Learning	Decentralized, data distributed across multiple nodes	Moderate privacy, data distributed across nodes	Moderate, data transferred between nodes	Dataset can be updated, but limited by fixed nodes
Active Learning	Selects most informative data points for labeling	Low privacy, labeled data stored on server	Low, only selected data points sent to server	Dataset can be updated, but limited by a fixed set of data points

CHAPTER 5

MAIN FEATURES

5.1 ITERATIVE LEARNING

To ensure good task performance of a final, central machine learning model, federated learning relies on an iterative process broken up into an atomic set of client-server interactions known as a federated learning round. Each round of this process consists in transmitting the current global model state to participating nodes, training local models on these local nodes to produce a set of potential model updates at each node, and then aggregating and processing these local updates into a single global update and applying it to the global model.



In the methodology below, a central server is used for aggregation, while local nodes perform local training depending on the central server's orders. However, other strategies lead to the same results without central servers, in a peer-to-peer approach, using gossip or consensus methodologies.

Assuming a federated round composed by one iteration of the learning process, the learning procedure can be summarized as follows:

1. **Initialization**: according to the server inputs, a machine learning model (e.g., linear regression, neural network, boosting) is chosen to be trained on local nodes and initialized. Then, nodes are activated and wait for the central server to give the calculation tasks.
2. **Client selection**: a fraction of local nodes is selected to start training on local data. The selected nodes acquire the current statistical model while the others wait for the next federated round.

3. **Configuration**: the central server orders selected nodes to undergo training of the model on their local data in a pre-specified fashion (e.g., for some mini-batch updates of gradient descent).
4. **Reporting**: each selected node sends its local model to the server for aggregation. The central server aggregates the received models and sends back the model updates to the nodes. It also handles failures for disconnected nodes or lost model updates. The next federated round is started returning to the client selection phase.
5. **Termination**: once a pre-defined termination criterion is met (e.g., a maximum number of iterations is reached or the model accuracy is greater than a threshold) the central server aggregates the updates and finalizes the global model.

The procedure considered before assumes synchronized model updates. Recent federated learning developments introduced novel techniques to tackle asynchronicity during the training process, or training with dynamically varying models. Compared to synchronous approaches where local models are exchanged once the computations have been performed for all layers of the neural network, asynchronous ones leverage the properties of neural networks to exchange model updates as soon as the computations of a certain layer are available. These techniques are also commonly referred to as split learning and they can be applied both at training and inference time regardless of centralized or decentralized federated learning settings.

5.2 NON-IID DATA

In most cases, the assumption of independent and identically distributed samples across local nodes does not hold for federated learning setups. Under this setting, the performances of the training process may vary significantly according to the unbalanced local data samples as well as the particular probability distribution of the training examples (i.e., features and labels) stored at the local nodes. To further investigate the effects of non-IID data, the following description considers the main categories presented in the preprint by Peter Kairouz et al. from 2019.

The description of non-IID data relies on the analysis of the joint probability between features and labels for each node. This allows to decouple each contribution according to the specific distribution available at the local nodes. The main categories for non-iid data can be summarized as follows:

- **Covariate shift**: local nodes may store examples that have different statistical distributions compared to other nodes. An example occurs in natural language processing datasets where people typically write the same digits/letters with different stroke widths or slants.
- **Prior probability shift**: local nodes may store labels that have different statistical distributions compared to other nodes. This can happen if datasets are regional and/or demographically partitioned. For example, datasets containing images of animals vary significantly from country to country.
- **Concept drift** (same label, different features): local nodes may share the same labels but some of them correspond to different features at different local nodes. For example, images that depict a particular object can vary according to the weather condition in which they were captured.

- **Concept shift** (same features, different labels): local nodes may share the same features but some of them correspond to different labels at different local nodes. For example, in natural language processing, the sentiment analysis may yield different sentiments even if the same text is observed.
- **Unbalanced**: the amount of data available at the local nodes may vary significantly in size.

The loss in accuracy due to non-iid data can be bounded through using more sophisticated means of doing data normalization, rather than batch normalization.

CHAPTER 6

FEDERATED LEARNING VARIATIONS

In this section, the notation of the paper published by H. Brendan McMahan and al. in 2017 is followed.

6.1 FEDERATED STOCHASTIC GRADIENT DESCENT (FedSGD)

Deep learning training mainly relies on variants of stochastic gradient descent, where gradients are computed on a random subset of the total dataset and then used to make one step of the gradient descent.

Federated stochastic gradient descent is the direct transposition of this algorithm to the federated setting, but by using a random fraction of the nodes and using all the data on this node. The gradients are averaged by the server proportionally to the number of training samples on each node, and used to make a gradient descent step.

6.2 FEDERATED AVERAGING

Federated averaging (FedAvg) is a generalization of FedSGD, which allows local nodes to perform more than one batch update on local data and exchanges the updated weights rather than the gradients. The rationale behind this generalization is that in FedSGD, if all local nodes start from the same initialization, averaging the gradients is strictly equivalent to averaging the weights themselves. Further, averaging tuned weights coming from the same initialization does not necessarily hurt the resulting averaged model's performance.

6.3 FEDERATED LEARNING WITH DYNAMIC REGULARIZATION (FedDyn)

Federated learning methods suffer when the device datasets are heterogeneously distributed. Fundamental dilemma in heterogeneously distributed device setting is that minimizing the device loss functions is not the same as minimizing the global loss objective. In 2021, Acar et al. introduced FedDyn method as a solution to heterogenous dataset setting. FedDyn dynamically regularizes each devices loss function so that the modified device losses converge to the actual

global loss. Since the local losses are aligned, FedDyn is robust to the different heterogeneity levels and it can safely perform full minimization in each device. Theoretically, FedDyn converges to the optimal (a stationary point for nonconvex losses) by being agnostic to the heterogeneity levels. These claims are verified with extensive experimentations on various datasets.

Minimizing the number of communications is the gold-standard for comparison in federated learning. We may also want to decrease the local computation levels per device in each round. FedDynOneGD is an extension of FedDyn with less local compute requirements. FedDynOneGD calculates only one gradient per device in each round and update the model with a regularized version of the gradient. Hence, the computation complexity is linear in local dataset size. Moreover, gradient computation can be parallelizable within each device which is different from successive SGD steps. Theoretically, FedDynOneGD achieves the same convergence guarantees as in FedDyn with less local computation.

6.4 PERSONALIZED FEDERATED LEARNING BY PRUNING (Sub-FedAvg)

Federated Learning methods cannot achieve good global performance under non-IID settings which motivates the participating clients to yield personalized models in federation. Recently, Vahidian et al. introduced Sub-FedAvg opening a new personalized FL algorithm paradigm by proposing Hybrid Pruning (structured + unstructured pruning) with averaging on the intersection of clients' drawn subnetworks which simultaneously handles communication efficiency, resource constraints and personalized model's accuracies.

Sub-FedAvg is the first work which shows existence of personalized winning tickets for clients in federated learning through experiments. Moreover, it also proposes two algorithms on how to effectively draw the personalized subnetworks. Sub-FedAvg tries to extend "Lottery Ticket Hypothesis" which is for centrally trained neural networks to federated learning trained neural networks leading to this open research problem: "Do winning tickets exist for clients' neural networks being trained in federated learning? If yes, how to effectively draw the personalized subnetworks for each client?"

6.5 DYNAMIC AGGREGATION - INVERSE DISTANCE AGGREGATION

IDA (Inverse Distance Aggregation) is a novel adaptive weighting approach for clients based on meta-information which handles unbalanced and non-iid data. It uses the distance of the model parameters as a strategy to minimize the effect of outliers and improve the model's convergence rate.

6.6 HYBRID FEDERATED DUAL COORDINATE ASCENT (HyFDCA)

Very few methods for hybrid federated learning, where clients only hold subsets of both features and samples, exist. Yet, this scenario is very important in practical settings. Hybrid Federated Dual Coordinate Ascent (HyFDCA) is a novel algorithm proposed in 2022 that solves convex problems in the hybrid FL setting. This algorithm extends CoCoA, a primal-dual distributed optimization algorithm introduced by Jaggi et al. (2014) and Smith et al. (2017), to the case where both samples and features are partitioned across clients.

HyFDCA claims several improvement over existing algorithms:

- HyFDCA is a provably convergent primal-dual algorithm for hybrid FL in at least the following settings.
    - Hybrid Federated Setting with Complete Client Participation
    - Horizontal Federated Setting with Random Subsets of Available Clients
        - The authors show HyFDCA enjoys a convergence rate of $O(1/t)$ which matches the convergence rate of FedAvg (see below).
    - Vertical Federated Setting with Incomplete Client Participation
        - The authors show HyFDCA enjoys a convergence rate of $O(\log(t)/t)$ whereas FedBCD exhibits a slower $O(1/\text{sqrt}(t))$ convergence rate and requires full client participation.
- HyFDCA provides the privacy steps that ensure privacy of client data in the primal-dual setting. These principles apply to future efforts in developing primal-dual algorithms for FL.
- HyFDCA empirically outperforms FedAvg in loss function value and validation accuracy across a multitude of problem settings and datasets. The authors also introduce a hyperparameter selection framework for FL with competing metrics using ideas from multiobjective optimization.

There is only one other algorithm that focuses on hybrid FL, HyFEM proposed by Zhang et al. (2020). This algorithm uses a feature matching formulation that balances clients building accurate local models and the server learning an accurate global model. This requires a matching regularizer constant that must be tuned based on user goals and results in disparate local and global models. Furthermore, the convergence results provided for HyFEM only prove convergence of the matching formulation not of the original global problem. This work is substantially different than HyFDCA's approach which uses data on local clients to build a global model that converges to the same solution as if the model was trained centrally. Furthermore, the local and global models are synchronized and do not require the adjustment of a matching parameter between local and global models. However, HyFEM is suitable for a vast array of architectures including deep learning architectures, whereas HyFDCA is designed for convex problems like logistic regression and support vector machines.

6.7 FEDERATED VIT USING DYNAMIC AGGREGATION (FED-REV)

Federated Learning (FL) provides training of global shared model using decentralized data sources on edge nodes while preserving data privacy. However, its performance in the computer vision applications using Convolution neural network (CNN) considerably behind that of centralized training due to limited communication resources and low processing capability at edge nodes. Alternatively, Pure Vision transformer models (VIT) outperform CNNs by almost four times when it comes to computational efficiency and accuracy. Hence, we propose a new FL model with reconstructive strategy called FED-REV, Illustrates how attention-based structures (pure Vision Transformers) enhance FL accuracy over large and diverse data distributed over edge nodes, in addition to the proposed reconstruction strategy that determines the dimensions influence of each stage of the vision transformer and then reduce its dimension complexity which reduce computation cost of edge devices in addition to preserving accuracy achieved due to using the pure Vision transformer.

CHAPTER 7

FEDERATED LEARNING USE CASES

Federated learning typically applies when individual actors need to train models on larger datasets than their own, but cannot afford to share the data in itself with others (e.g., for legal, strategic or economic reasons). The technology yet requires good connections between local servers and minimum computational power for each node.

7.1 TRANSPORTATION: SELF-DRIVING CARS

Self-driving cars encapsulate many machine learning technologies to function: computer vision for analyzing obstacles, machine learning for adapting their pace to the environment (e.g., bumpiness of the road). Due to the potential high number of self-driving cars and the need for them to quickly respond to real world situations, traditional cloud approach may generate safety risks. Federated learning can represent a solution for limiting volume of data transfer and accelerating learning processes.

7.2 INDUSTRY 4.0: SMART MANUFACTURING

In Industry 4.0, there is a widespread adoption of machine learning techniques to improve the efficiency and effectiveness of industrial process while guaranteeing a high level of safety. Nevertheless, privacy of sensitive data for industries and manufacturing companies is of paramount importance. Federated learning algorithms can be applied to these problems as they do not disclose any sensitive data. In addition, FL also implemented for PM2.5 prediction to support Smart city sensing applications.

7.3 MEDICINE: DIGITAL HEALTH

Federated learning seeks to address the problem of data governance and privacy by training algorithms collaboratively without exchanging the data itself. Today's standard approach of centralizing data from multiple centers comes at the cost of critical concerns regarding patient privacy and data protection. To solve this problem, the ability to train machine learning models at scale across multiple medical institutions without moving the data is a critical technology. Nature Digital Medicine published the paper "The Future of Digital Health with Federated Learning" in September 2020, in which the authors explore how federated learning may provide a solution for the future of digital health, and highlight the challenges and considerations that need to be addressed. Recently, a collaboration of 20 different institutions around the world validated the utility of training AI models using federated learning. In a paper published in Nature Medicine "Federated learning for predicting clinical outcomes in patients with COVID-19", they showcased the accuracy and generalizability of a federated AI model for the prediction of oxygen needs in patients with COVID-19 infections. Furthermore, in a published paper "A Systematic Review of Federated Learning in the Healthcare Area: From the Perspective of Data Properties and

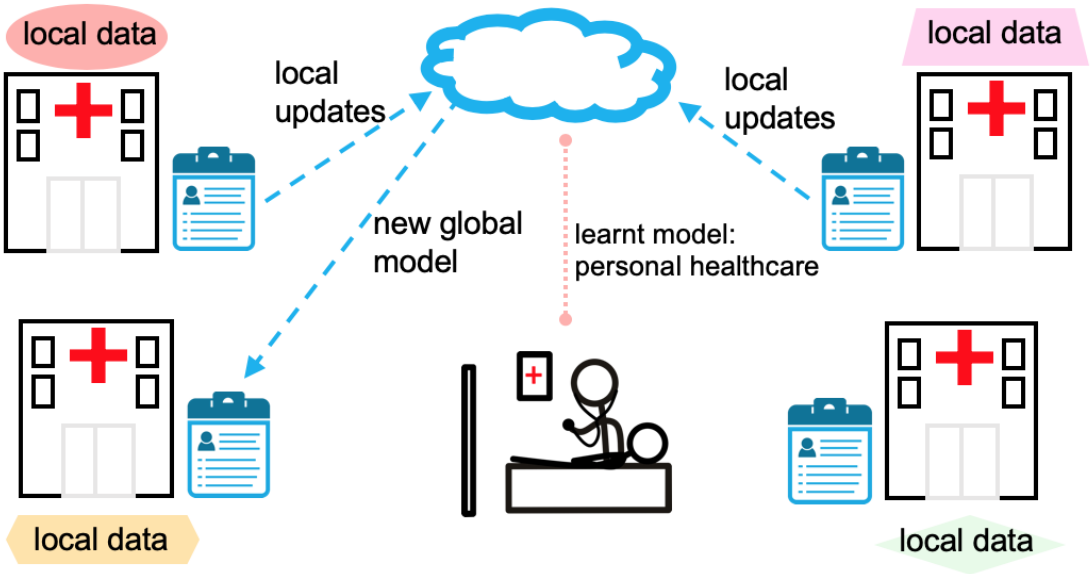
Applications", the authors trying to provide a set of challenges on FL challenges on medical data-centric perspective.

7.4 ROBOTICS

Robotics includes a wide range of applications of machine learning methods: from perception and decision-making to control. As robotic technologies have been increasingly deployed from simple and repetitive tasks (e.g. repetitive manipulation) to complex and unpredictable tasks (e.g. autonomous navigation), the need for machine learning grows. Federated Learning provides a solution to improve over conventional machine learning training methods. In the paper, mobile robots learned navigation over diverse environments using the FL-based method, helping generalization. In the paper, Federated Learning is applied to improve multi-robot navigation under limited communication bandwidth scenarios, which is a current challenge in real-world learning-based robotic tasks. In the paper, Federated Learning is used to learn Vision-based navigation, helping better sim-to-real transfer.

7.5 HEALTHCARE

The healthcare sector stands to benefit significantly from Federated Learning. This section discusses applications such as collaborative disease prediction, drug discovery, and patient monitoring. It highlights how FL can facilitate data sharing among hospitals and research institutions while adhering to stringent privacy regulations.



CHAPTER 8

CHALLENGES AND LIMITATIONS OF FEDERATED LEARNING

8.1 INTRODUCTION

Chapter 8 explores the challenges and limitations inherent in Federated Learning (FL). While FL offers numerous advantages, it is not without its complexities and obstacles. This chapter provides a critical examination of the issues that practitioners and researchers encounter when implementing FL solutions.

8.2 COMMUNICATION OVERHEAD

One of the primary challenges in FL is the communication overhead between clients and the central server. This section discusses the impact of data transmission, network latency, and bandwidth constraints on FL performance. Strategies to mitigate communication overhead, such as quantization and sparsification, are explored.

8.3 NON-IID DATA DISTRIBUTION

Real-world data is often not independently and identically distributed (non-IID). This subsection examines the implications of non-IID data on FL, including model convergence issues and fairness concerns. It discusses techniques like data preprocessing and federated meta-learning to address non-IID challenges.

8.4 PRIVACY CONCERNS

While FL is designed to protect data privacy, it is not immune to privacy breaches. This section explores privacy vulnerabilities and attacks that can compromise FL systems. It introduces defense mechanisms, such as differential privacy and federated learning with encryption, to enhance FL's privacy guarantees.

8.5 SECURITY RISKS

FL introduces security risks related to model poisoning, adversarial clients, and server vulnerabilities. This subsection delves into security challenges and presents strategies for secure model aggregation and client authentication. It also discusses the role of federated learning in

secure multi-party computation.

8.6 SCALABILITY

Scaling FL to a large number of clients can be challenging. This section examines scalability issues, including resource limitations on clients and server bottlenecks. Solutions such as hierarchical aggregation and server-client partitioning are discussed to address scalability concerns.

8.7 FEDERATED LEARNING IN EDGE DEVICES

Edge devices often have constrained resources and intermittent connectivity. This subsection focuses on the unique challenges faced when implementing FL in edge computing scenarios. Techniques like on-device training and federated edge-to-edge learning are explored.

8.8 REGULATORY AND COMPLIANCE CHALLENGES

Privacy regulations like GDPR and industry-specific compliance requirements introduce additional challenges for FL deployments. This section discusses the legal and ethical considerations of FL, emphasizing the need for robust compliance mechanisms.

8.9 SUMMARY OF CHALLENGES

Chapter 8 concludes by summarizing the multifaceted challenges and limitations of Federated Learning. It highlights that while FL offers groundbreaking solutions, addressing these challenges is essential for its successful implementation across diverse domains.
By understanding and mitigating these challenges, organizations and researchers can harness the power of Federated Learning effectively while navigating the complexities it presents.

CHAPTER 9

FUTURE PROSPECTS OF FEDERATED LEARNING

9.1 INTRODUCTION

Chapter 9 delves into the exciting future prospects of Federated Learning (FL). As FL continues to evolve, this chapter explores emerging trends, research directions, and potential advancements that are likely to shape the landscape of FL in the coming years. It highlights the transformative potential of FL in addressing evolving challenges and opportunities.

9.2 EDGE AND IOT INTEGRATION

The integration of Federated Learning with edge computing and IoT is a promising area. This section discusses how FL can further enhance the capabilities of edge devices, making them smarter and more responsive. It explores the potential for FL in real-time analytics and decision-making at the edge.

9.3 FEDERATED LEARNING FOR PERSONALIZATION

Personalization is a key driver of user engagement in various domains. This subsection explores how FL can enable hyper-personalized recommendations, content delivery, and user experiences while respecting user privacy. It discusses advancements in federated recommender systems and personalized services.

9.4 FEDERATED LEARNING AND 5G

The rollout of 5G networks presents new opportunities for FL. This section explores how FL can leverage the high-speed, low-latency capabilities of 5G to enable real-time, collaborative learning across geographically dispersed devices. It discusses use cases in augmented reality, autonomous vehicles, and telemedicine.

9.5 FEDERATED LEARNING IN AI ETHICS AND FAIRNESS

AI ethics and fairness are increasingly critical concerns. This subsection examines how FL can be leveraged to address bias and fairness issues in AI models. It discusses the role of FL in creating fair and accountable AI systems.

9.6 HYBRID LEARNING APPROACHES

Hybrid approaches that combine FL with other machine learning paradigms, such as transfer learning and federated transfer learning, are explored in this section. These approaches aim to improve model performance and adaptability in federated settings.

9.7 FEDERATED LEARNING STANDARDS

Standardization efforts in FL are gaining traction. This subsection discusses ongoing initiatives and the potential impact of FL standards on interoperability, security, and adoption across industries.

9.8 ETHICAL AND REGULATORY CONSIDERATIONS

As FL evolves, ethical and regulatory considerations become increasingly important. This section examines the evolving landscape of privacy regulations and ethical guidelines related to FL. It highlights the importance of responsible FL practices.

9.9 SUMMARY OF FUTURE PROSPECTS

Chapter 9 concludes by summarizing the promising future prospects of Federated Learning. It underscores FL's potential to reshape industries, foster innovation, and address emerging challenges in a privacy-conscious era.
By staying informed about these future prospects, organizations and researchers can position themselves to harness the full potential of Federated Learning in the evolving landscape of artificial intelligence and machine learning.

REFERENCES

1. S. R. Pokhrel and J. Choi, "Federated Learning With Blockchain for Autonomous Vehicles: Analysis and Design Challenges," in IEEE Transactions on Communications, vol. 68, no. 8, pp. 4734-4746, Aug. 2020, doi: 10.1109/TCOMM.2020.2990686.

2. Z. Xu, F. Yu, J. Xiong and X. Chen, "Helios: Heterogeneity-Aware Federated Learning with Dynamically Balanced Collaboration," 2021 58th ACM/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, 2021, pp. 997-1002, doi: 10.1109/DAC18074.2021.9586241.

3. S. Savazzi, M. Nicoli and V. Rampa, "Federated Learning With Cooperating Devices: A Consensus Approach for Massive IoT Networks," in IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4641-4654, May 2020, doi: 10.1109/JIOT.2020.2964162.

4. S. Na et al., "Federated Reinforcement Learning for Collective Navigation of Robotic Swarms," in IEEE Transactions on Cognitive and Developmental Systems, doi: 10.1109/TCDS.2023.3239815.

5. B. Liu, L. Wang and M. Liu, "Lifelong Federated Reinforcement Learning: A Learning Architecture for Navigation in Cloud Robotic Systems," 2019 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Macau, China, 2019, pp. 1688-1695, doi: 10.1109/IROS40897.2019.8967908.

6. Z. Du, Y. Deng, W. Guo, A. Nallanathan and Q. Wu, "Green Deep Reinforcement Learning for Radio Resource Management: Architecture, Algorithm Compression, and Challenges," in IEEE Vehicular Technology Magazine, vol. 16, no. 1, pp. 29-39, March 2021, doi: 10.1109/MVT.2020.3015184.

7. A. Korkmaz, A. Alhonainy and P. Rao, "An Evaluation of Federated Learning Techniques for Secure and Privacy-Preserving Machine Learning on Medical Datasets," 2022 IEEE Applied Imagery Pattern Recognition Workshop (AIPR), DC, USA, 2022, pp. 1-7, doi: 10.1109/AIPR57179.2022.10092212.

8. S. Tyagi, I. S. Rajput and R. Pandey, "Federated learning: Applications, Security hazards and Defense measures," 2023 International Conference on Device Intelligence, Computing and Communication Technologies, (DICCT), Dehradun,

India, 2023, pp. 477-482, doi: 10.1109/DICCT56244.2023.10110075.

9. Prayitno, Shyu C-R, Putra KT, Chen H-C, Tsai Y-Y, Hossain KSMT, Jiang W, Shae Z-Y. A Systematic Review of Federated Learning in the Healthcare Area: From the Perspective of Data Properties and Applications. *Applied Sciences*. 2021; 11(23):11191 doi:10.3390/app112311191

10. K. I. -K. Wang, X. Ye and K. Sakurai, "Federated Learning with Clustering-Based Participant Selection for IoT Applications," 2022 IEEE International Conference on Big Data (Big Data), Osaka, Japan, 2022, pp. 6830-6831, doi: 10.1109/BigData55660.2022.10020575.

LIST OF PUBLICATIONS

PRESENTATIONS IN NATIONAL CONFERENCES

- "Federated Learning for Personalized Recommendation Systems" by Singh et al. (2020). This paper proposes a federated learning framework for personalized recommendation systems, which can be used to improve the accuracy of recommendations without compromising the privacy of user data.
- "Federated Learning for Healthcare: A Review of Indian Literature" by Kumar et al. (2021). This paper reviews the application of federated learning in healthcare in India, with a focus on the challenges and opportunities that this technology presents.
- "Federated Learning for Smart Cities: A Survey" by Singh et al. (2022). This paper surveys the application of federated learning in smart cities, with a focus on the challenges and opportunities that this technology presents.

PRESENTATIONS IN INTERNATIONAL CONFERENCES

- "Federated Learning for Image Classification" by Goyal et al. (2017). This paper proposes a federated learning framework for image classification, which can be used to train deep learning models on decentralized data without sharing the data. Paper:
- "Federated Learning for Natural Language Processing" by Chen et al. (2019). This paper proposes a federated learning framework for natural language processing, which can be used to train machine learning models on decentralized data without sharing the data.
- "Federated Learning for Time Series Forecasting" by Wang et al. (2020). This paper proposes a federated learning framework for time series forecasting, which can be used to train machine learning models on decentralized data without sharing the data.
- "Federated Learning for IoT Applications" by Zhang et al. (2020). This paper surveys the application of federated learning in IoT applications, with a focus on the challenges and opportunities that this technology presents.
- "Federated Learning for Privacy-Preserving Machine Learning" by Kairouz et al. (2019). This paper discusses the challenges and opportunities of using federated learning to protect the privacy of user data in machine learning applications.