Kenan Stredic
Federated Machine Learning Summary

Links:

https://flower.dev/docs/framework/tutorial-quickstart-pytorch.html
https://flower.dev/docs/framework/example-walkthrough-pytorch-mnist.html
https://flower.dev/docs/framework/tutorial-series-what-is-federated-learning.html
https://flower.dev/docs/
https://flower.dev/conf/flower-summit-2023/
https://arxiv.org/pdf/1902.04885.pdf
https://arxiv.org/pdf/1909.11875.pdf

Federated Machine Learning: Concept, Applications, and Business Model

1. Introduction

Federated learning is introduced as an innovative approach enabling the collaborative construction of machine learning models across multiple parties while preserving the privacy of their training data. The technology addresses challenges related to data privacy and security, making it particularly relevant in various industries where direct data aggregation is restricted.

2. Basic Concepts and Architecture

The fundamental concepts and architecture of federated learning are discussed. The federated learning process involves decentralized model training across multiple devices or servers, emphasizing privacy-preserving techniques. The architecture includes a central server coordinating model updates from participating devices while respecting data privacy constraints.

3. Related Works

Federated learning is positioned in relation to other concepts, such as privacy-preserving machine learning, distributed machine learning, edge computing, and federated database systems. Privacy-preserving machine learning encompasses secure multi-party computation techniques. Federated learning is compared to distributed machine learning, addressing issues like non-IID data. It is also related to edge computing, acting as an operating system, and shares similarities with federated database systems regarding data types and storage.

4. Applications

The applications of federated learning span various industries, including sales and finance. In smart retail, federated learning addresses challenges of scattered data across departments, offering privacy protection and personalized services. It is applied in finance to detect multi-party borrowing without exposing user lists. Smart healthcare stands to benefit by uniting medical institutions and sharing data through federated learning, enhancing machine learning model performance.

5. Federated Learning and Data Alliance of Enterprises

Federated learning is not just a technology standard but also a business model. It challenges the traditional cloud computing model by allowing institutions to share a united model without data exchange, promoting equitable profit allocation through consensus mechanisms. The concept of data alliances is introduced, where data possessors are motivated to join, irrespective of data scale, ensuring fair profit distribution.

6. Conclusions and Prospects

Federated learning emerges as a solution to challenges posed by data isolation and privacy concerns in the AI era. It enables the creation of united models while safeguarding local data, fostering collective benefits for enterprises. The article anticipates that federated learning will transcend industry barriers, creating a community for secure data and knowledge sharing. The ultimate vision is to bring the benefits of artificial intelligence to every aspect of life, with a focus on fairness and contribution-based profit distribution.

Kenan Stredic
Federated Machine Learning Summary

Federated Learning in Mobile Edge Networks: A Comprehensive Survey

Chapter I: INTRODUCTION

- Overview: Federated Learning (FL) is introduced as a paradigm where machine learning models are trained across decentralized devices without centralizing raw data. This mitigates privacy concerns and allows for collaborative model training.
- Challenges: The introduction highlights key challenges in FL, such as high communication costs, model heterogeneity across devices, and privacy preservation.
- Objectives: The goals include scaling FL to large and diverse networks, optimizing communication for efficiency, and ensuring robust model convergence.

Chapter II: FEDERATED LEARNING BASICS

- Definition: FL is defined as a decentralized machine learning approach where the training process occurs locally on client devices, and only model updates are communicated to a central server.
- Key Components:
  - Clients (Devices): Local devices that possess data but do not share it directly. They perform local training.
  - Server: Centralized entity that aggregates model updates from clients and disseminates the global model.
  - Global Model: The overarching model updated through collaboration with all clients.
- Process: FL operates iteratively, with clients training on their local data, sending model updates to the server, and the server aggregating these updates to refine the global model.

Chapter III: COMMUNICATION COST REDUCTION IN FEDERATED LEARNING

- Challenges: Communication costs in FL are addressed, focusing on issues like the high dimensionality of updates, unreliable network conditions, and asymmetry in internet connection speeds.
- Strategies:

- Edge and End Computation: Increasing computation on edge devices to reduce communication rounds. This involves more parallelism or computation per participant before global aggregation.
- Model Compression: Techniques like structured updates (low-rank and random mask), sketched updates (subsampling, quantization), and federated dropout to reduce the size of communicated updates.
- Importance-based Updating: Algorithms like eSGD (edge Stochastic Gradient Descent) that selectively communicate important gradients, considering sparsity in DNN models.
- Lessons Learned: Recognizes tradeoffs between communication cost reduction and model accuracy. Calls for theoretical optimization and suggests inspiration from Mobile Edge Computing (MEC) paradigm. Acknowledges the need for further exploration, especially regarding device heterogeneity.

These chapters provide a comprehensive introduction to FL, cover its foundational components, and delve into strategies for mitigating communication costs, a crucial consideration for FL implementation.

Chapter IV: Incentive Mechanism, Reputation, and Lessons Learned

Incentive Mechanism:
- Service Pricing Scheme: Participants act as training service providers in a Stackelberg game. Model updates are traded cooperatively, ensuring uniqueness of Stackelberg equilibrium and energy-efficient communication. Challenges include limited involvement of mobile devices [141].

- DRL-Based Approach: Combines Stackelberg game with Deep Reinforcement Learning (DRL). FL server acts as an agent optimizing payment, while edge nodes determine participation levels. Enables dynamic incentive policy adaptation without prior information [145].

- Contract Theoretic Approach: Contracts designed for varying data qualities reduce information asymmetry. Ensures Individual Rationality (IR) and Incentive Compatibility (IC). Extracts more profits from participants compared to Stackelberg game approach [146].

- Reputation-Based Scheme: Introduces reputation metric, derived from direct and indirect opinions. Uses a decentralized reputation blockchain for secure management. Participants with reputation above a threshold are selected for FL training, improving model accuracy [146].

Summary and Lessons Learned:
- Resource Allocation Considerations:
- Efficient FL requires addressing challenges like the straggler effect and varying data quality.

- Heterogeneous resources (computation, communication, willingness to participate) are crucial considerations.
- Tools like DRL and contract theory help optimize resource allocation in dynamic network conditions.

- Tradeoffs in Resource Allocation:
  - Communication cost reduction may impact computation costs or inference accuracy.
  - Scalable models allow customization to balance competing needs, e.g., fairness calibration or tradeoffs in completion time and energy expense.

- Challenges in Synchronous and Asynchronous FL:
  - Synchronous FL susceptible to straggler effect; asynchronous FL allows joining midway but faces convergence delays.
  - Despite advantages, asynchronous FL isn't widely adopted due to convergence guarantees.

- Incentive Mechanism Design:
  - Incentivizing contributions from participants is crucial.
  - Studies explore service pricing, DRL-based approaches, contract theory, and reputation-based schemes.
  - Limitations include assumptions of a federation monopoly, neglecting competition among data owners or FL servers.

- Privacy and Security Considerations:
  - Assumption of FL ensuring privacy and security; potential challenges discussed in the following section.
  - Malicious participants or FL servers may compromise privacy and security.

Chapter V: Privacy and Security Issues

The chapter delves into diverse incentive mechanisms and resource allocation strategies, emphasizing the importance of addressing heterogeneity, tradeoffs, and privacy concerns in FL systems.

Chapter V of the document discusses privacy and security issues in Federated Learning (FL). The main objectives of FL include protecting the privacy of participants by sharing only the model parameters rather than raw data. However, the chapter explores how privacy and security concerns can arise, particularly when participants or FL servers are malicious. The key issues discussed are privacy and security, and the chapter covers the following aspects:

Privacy Issues

1. Information Exploiting Attacks in Machine Learning
   - Discusses the possibility of extracting information from a trained model.

Kenan Stredic
Federated Machine Learning Summary

- Highlights the risk of inferring sensitive information like ethnicity or gender from shared models.
- Provides examples of model-inversion algorithms and model extraction attacks.

2. Differential Privacy-Based Protection Solutions for FL Participants
- Introduces differentially private stochastic gradient descent to add noise to trained parameters.
- Proposes an approach for better privacy protection, including selecting random participants for training.

3. Collaborative Training Solutions
- Discusses collaborative DL frameworks where participants selectively share parameters.
- Introduces federated GANs to generate artificial data, reducing the risk of malicious exploitation.
- Highlights the vulnerability of selective parameter sharing and DP solutions to powerful attacks.

4. Encryption-Based Solutions
- Introduces homomorphic encryption to protect shared parameters from curious servers.
- Discusses hybrid solutions combining homomorphic encryption and DP for improved privacy.

Security Issues:

1. Data Poisoning Attacks
- Describes how malicious participants can poison the global model by creating dirty-label data.
- Introduces FoolsGold as a defense strategy to distinguish honest participants from potential attackers.

2. Model Poisoning Attacks
- Explores model poisoning attacks, where a malicious participant directly poisons the shared global model.
- Suggests solutions based on checking the effectiveness of shared models and comparing updated models.

3. Free-Riding Attacks
- Discusses free-riding attacks, where participants benefit from the global model without contributing.
- Introduces a blockchain-based FL architecture (BlockFL) to prevent free-riding and incentivize contributions.

Summary and Lessons Learned:

Kenan Stredic
Federated Machine Learning Summary

- FL is considered an effective privacy-preserving solution, but the chapter highlights potential risks and attacks.
- Malicious participants can exploit the FL process, leading to information leakage and falsified model updates.
- Countermeasures such as differential privacy, collaborative training, encryption, and blockchain-based architectures are discussed to address privacy and security concerns.

The summary emphasizes the importance of understanding and mitigating privacy and security issues to guide FL system administrators in implementing appropriate countermeasures. The chapter concludes by summarizing key information about attacks and their corresponding countermeasures.

Chapter VI: Applications

This chapter discusses various applications of Federated Learning (FL) for optimizing mobile edge networks. Here's a detailed summary of the content:

Overview:
The text explores the use of Federated Learning (FL) as an enabling technology for collaborative learning at mobile edge networks. It emphasizes the application of FL in optimizing mobile edge networks, addressing the challenges related to privacy issues associated with user data.

Applications of FL in Mobile Edge Computing:
1. Cyberattack Detection:
  - DL (Deep Learning) has been successful in cyberattack detection.
  - FL is proposed to collaboratively train cyberattack detection models while preserving user privacy.
  - Techniques such as differentially private stochastic gradient descent are introduced to address privacy concerns.

2. Edge Caching and Computation Offloading:
  - FL is applied to optimize decisions related to caching and computation offloading in Mobile Edge Computing (MEC) systems.
  - DRL (Deep Reinforcement Learning) with FL is used to make decisions regarding file caching and computation offloading based on user equipment states.
  - Privacy is maintained by training with data remaining on user devices, and FL algorithms like FedAvg are employed for robust training.

3. Base Station Association:
  - In dense networks, optimizing base station association is crucial to limit interference faced by users.

Kenan Stredic
Federated Machine Learning Summary

- FL is suggested as an approach to optimize base station association while considering user privacy constraints.

4. Vehicular Networks:
- FL is applied to vehicular networks for tasks such as traffic queue length prediction and energy demand in electric vehicle charging stations.
- Extreme Value Theory (EVT) is proposed for rare events prediction, and FL is used to enable collaborative learning while ensuring privacy.
- For energy demand learning in charging stations, Federated Energy Demand Learning (FEDL) is introduced, where FL is employed to manage energy resources while maintaining user privacy.

Privacy-Preserving Techniques:
- Information Exploiting Attacks (Privacy Issues):
- Different techniques such as differentially private stochastic gradient descent and secret sharing schemes are introduced to address privacy issues in FL.

- Data Poisoning Attacks:
- Techniques like FoolsGoal are presented to detect and mitigate attacks where attackers poison the global model by creating dirty-label data.

- Model Poisoning Attacks:
- Methods for detecting and preventing direct poisoning of the global model sent to the server are discussed.

- Free-Riding Attacks:
- An approach called BlockFL is suggested to prevent participants from benefiting from the global model without contributing to the learning process.

FL-Based Approaches for Mobile Edge Network Optimization:
- The text provides a summary of FL-based approaches for different applications, including cyberattack detection, edge caching, computation offloading, base station association, and vehicular networks.
- It mentions specific references for each application, detailing the proposed techniques and their advantages.

Conclusion:
The section concludes by summarizing that FL, combined with various machine learning approaches, can be effectively used for optimizing mobile edge networks while addressing privacy concerns associated with sensitive user data. It highlights the importance of FL in enabling collaborative learning and privacy-preserving applications in edge computing.

Kenan Stredic

Chapter VII: Challenges and Future Research Directions

In Chapter VII, the text discusses challenges and future research directions in the deployment of Federated Learning (FL) at scale. Here's a summarized breakdown of the key points:

1. Dropped Participants:
   - Challenge: Participants may go offline, impacting FL system performance.
   - Solution: Provide dedicated connections to avoid dropouts.

2. Privacy Concerns:
   - Challenge: Model updates during training may expose sensitive information.
   - Solutions: Use privacy-preserving techniques like Differential Privacy (DP), but balance with performance considerations.

3. Unlabeled Data:
   - Challenge: Data in federated networks may be unlabeled or mislabeled.
   - Solution: Enable devices to construct labeled data from each other, consider semi-supervised learning.

4. Interference Among Mobile Devices:
   - Challenge: Geographically close devices may interfere during model updates.
   - Solution: Combine channel and resource allocation approaches, explore data-driven solutions like federated Deep Reinforcement Learning (DRL).

5. Communication Security:
   - Challenge: FL is vulnerable to communication security issues like jamming attacks.
   - Solution: Adopt anti-jamming schemes like frequency hopping.

6. Asynchronous FL:
   - Challenge: Synchronous FL is susceptible to the straggler effect.
   - Solution: Explore asynchronous FL for scalability, consider convergence guarantees in non-IID settings.

7. Comparisons with Other Methods:
   - Challenge: Privacy-preserving distributed learning methods like split learning are compared with FL.
   - Consideration: Research efforts needed to guide administrators on choosing the appropriate learning method.

8. Learning Convergence:
   - Challenge: Convergence of FL algorithms is not guaranteed.

- Research Direction: Explore convergence guarantees for non-convex loss functions in non-IID settings.

9. Quantifying Statistical Heterogeneity:
- Challenge: Mobile devices generate non-IID data, and quantifying statistical heterogeneity is essential for FL convergence.
- Research Direction: Develop efficient algorithms for quick determination of heterogeneity in federated networks.

10. Combined Algorithms for Communication Reduction:
- Challenge: Explore how techniques for communication reduction in FL can be combined.
- Consideration: Evaluate tradeoffs between accuracy and communication overhead.

11. Cooperative Mobile Crowd ML:
- Challenge: Direct communication between devices and the server increases energy consumption.
- Solution: Use cluster heads for relay in Device-to-Device connections, improving energy efficiency.

12. Applications of FL:
- Consideration: FL has applications in healthcare, finance, and transport systems.
- Research Direction: Future studies should address specific implementation challenges in different application scenarios.

In Chapter VIII, the conclusion summarizes the tutorial on FL, provides insights into FL's role in Mobile Edge Computing (MEC), discusses fundamentals, reviews implementation challenges, and outlines future research directions.