BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI

A Report

On

Federated Learning

Submitted To:

Prof. Navneet Goyal
Professor,
Department of Computer Science and Information Systems,
BITS Pilani

Submitted By:

Group 03
Arjoo Kumari (2020B3A70770P)
Adarsh Goel (2020B3A70821P)

1. Introduction

The traditional notions of centralized model training are being redefined in the ever-changing landscape of machine learning. This rapid growth of data has highlighted the need for innovative strategies that balance powerful model development with individual data protection, especially in the era of IoT and ubiquitous computing. As a groundbreaking solution, Federated Learning offers a decentralized framework that enables local device-based model training without the exchange of sensitive data. Its emergence marks a transformative paradigm for privacy-sensitive model training.

In essence, Federated Learning tackles the dilemma of using vast datasets to enhance models whilst safeguarding users' private details. The usual method of machine learning entails gathering data in one central location, a practice that frequently sparks worries regarding the ownership, security, and confidentiality of data. However, Federated Learning avoids such issues by distributing the process of model training among numerous gadgets, allowing cooperation without infringing on personal privacy.

Preserving user data locally is the cornerstone of Federated Learning. Instead of sending personal information to a central server, just updates, usually in the form of gradients, go through the network. This approach ensures that sensitive data stays on the user's device. It's a new way of thinking about privacy-conscious technologies.

From healthcare to smart grids and mobile applications, the impact of Federated Learning has been felt across diverse domains. Its ability to facilitate collaborative model training while preserving privacy has stimulated research, innovation, and practical implementations. This report scrutinizes the specificities of Federated Learning, including its essential notions, intricate architecture, obstacles, uses, and the direction it steers machine learning towards in a world that puts a high regard on safeguarding personal data privacy.

2. Key Concepts

a. Decentralized Training

At the heart of Federated Learning (FL) lies the concept of decentralized training, a departure from the conventional model where data is centralized for processing. In FL, model training occurs locally on individual devices, such as smartphones, IoT gadgets, or servers, eliminating the need for raw data to leave its source. This decentralized approach is pivotal in addressing privacy concerns associated with centralized models, as it ensures that sensitive information remains localized and under the control of the data owner. The decentralized training process involves a synchronization mechanism where local

devices collaboratively train a global model without sharing raw data. Each device computes updates to the model based on its local data, typically in the form of gradients. These updates are then transmitted to a central server, which aggregates them to refine the global model. This iterative process allows the model to learn from the collective knowledge of all participating devices while preserving the privacy of individual datasets.

b. Privacy Preservation

One of the primary motivations behind the rise of FL is its unwavering commitment to privacy preservation. In traditional machine learning setups, the amalgamation of data in centralized repositories poses inherent risks to individual privacy. FL tackles this challenge by keeping user data on their respective devices. The only information transmitted to the central server is the model update, an abstract representation of the knowledge gained during local training.
By design, FL minimizes the exposure of sensitive data, mitigating the potential for data breaches or unauthorized access. This approach not only aligns with evolving data protection regulations but also instills confidence among users wary of sharing personal information. Privacy-preserving techniques, such as federated averaging and secure aggregation, play a crucial role in ensuring that the collaborative model training process does not compromise the confidentiality of individual datasets.

c. Communication Protocols

The success of FL hinges on effective communication protocols that enable the secure and efficient transmission of model updates between local devices and the central server. Given the sensitivity of the transmitted information, protocols must be designed to protect against eavesdropping, tampering, or any form of malicious activity during data exchange. Techniques such as secure multi-party computation (SMPC), homomorphic encryption, and differential privacy are integral to FL communication protocols. Secure aggregation, a method where model updates are aggregated without exposing individual contributions, is a common practice. These protocols collectively ensure the integrity and confidentiality of the data in transit, fortifying the overall security posture of FL systems.

3. Architecture

a. Central Server

The architectural foundation of Federated Learning revolves around a central server that orchestrates the collaborative model training process. This central entity plays a pivotal

role in aggregating model updates from the diverse array of participating local devices and computing the global model. The server acts as a nexus for communication, receiving the distilled insights from individual devices and disseminating the refined model parameters back to the network. The central server's responsibilities include maintaining synchronization among the local models, initiating the aggregation process, and disseminating the updated global model to all contributing devices. While the server is integral to the FL architecture, it does not possess direct access to the raw data residing on individual devices, aligning with the core tenet of privacy preservation in FL.

b. Local Devices

At the periphery of the FL architecture are the local devices, which can encompass a diverse range of endpoints such as smartphones, IoT devices, or servers. These devices house the raw data and perform local model training based on their specific datasets. The local models undergo iterative refinement, generating updates that encapsulate the insights gleaned from the local data. It is important to note that the local devices in FL are not mere data contributors; they are active participants in the model training process. Each device computes its model updates independently, contributing nuanced information based on its unique dataset. The updates are then transmitted to the central server for aggregation. This decentralized approach empowers devices at the edge of the network, promoting a collaborative learning paradigm without compromising data privacy.

c. Communication Protocols

The linchpin of the FL architecture is the intricate web of communication protocols that facilitate the seamless exchange of information between the central server and local devices. The transmission of model updates requires careful consideration of security, efficiency, and privacy. Several key communication protocols and techniques contribute to the robustness of FL systems:

a) Secure Aggregation: To protect against eavesdropping and tampering, secure aggregation is employed. This technique ensures that model updates are aggregated in a way that individual contributions remain confidential, enhancing the overall privacy of the FL process.
b) Differential Privacy: By introducing noise or randomness to the model updates, differential privacy further fortifies the privacy guarantees of FL. It prevents the reconstruction of individual data points from the aggregated updates, adding an extra layer of protection.

c) Encryption and Authentication: The transmission of model updates is often secured through encryption and authentication mechanisms, safeguarding against unauthorized access and ensuring the integrity of the transmitted data.

These communication protocols collectively establish a secure and efficient channel for the exchange of information, reinforcing the privacy-centric architecture of FL.

The architecture of Federated Learning, characterized by the symbiotic relationship between the central server and local devices, exemplifies a novel approach to collaborative model training. The orchestration of decentralized processes, coupled with robust communication protocols, positions FL as a pioneering paradigm that reconciles the imperatives of machine learning advancement with the paramount importance of individual data privacy.

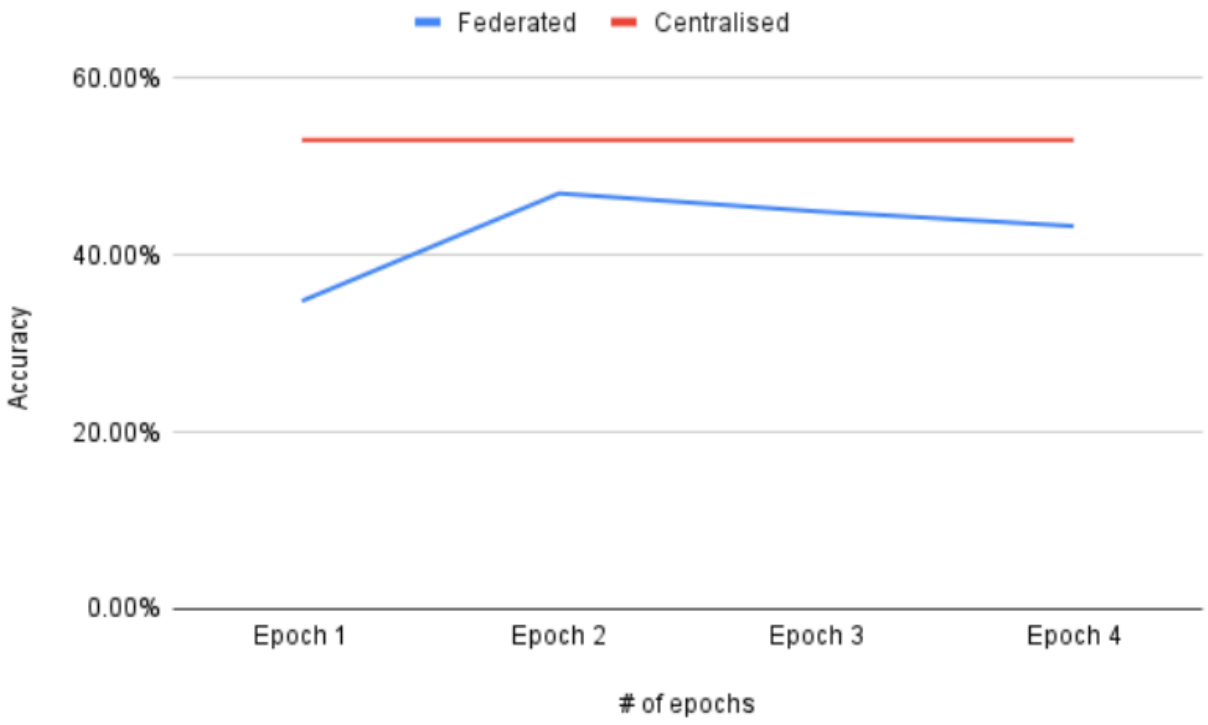
4. Our Implementation

We utilized a simple CNN (Convoluted Neural Network) for centralized and federated learning. The clients were represented as files with their meta data having details regarding battery percentage, battery time remaining, whether data is modified or not and total number of images.

There are three classes in our animal classifier namely: cat, dog and pandas. We took the dataset from https://www.kaggle.com/code/bygbrains/dog-cat-pandas-image-classifier/input. We utilized the complete dataset for centralized learning and divided the dataset for each user in each round for federated learning.

5. Result

The training accuracy for centralized learning is 53.03% and the training accuracy for the federated learning is 43.30%. The test accuracy for centralized learning is 47.67% and for the federated learning is 41.33%. The training time for centralized learning was 23 minutes and for the federated learning is 32 minutes. The difference in time can be attributed to communication cost. The following graph shows the results for training on federated learning during the 4 rounds.



6. Challenges

a. Heterogeneity

Federated Learning operates in a real-world environment where participating devices exhibit diverse characteristics in terms of hardware capabilities, network conditions, and data distributions. This heterogeneity poses a significant challenge to FL systems. Developing algorithms that can adapt and effectively leverage contributions from devices with disparate capabilities and data profiles is an ongoing area of research. Addressing this challenge is crucial for ensuring the scalability and performance of FL across a wide range of devices and networks.

b. Security Concerns

While Federated Learning offers a privacy-preserving framework, it introduces new security challenges. The communication between local devices and the central server is a potential target for adversaries seeking to compromise the integrity of the model or glean insights into individual datasets. Protecting against adversarial attacks, ensuring the authenticity of model updates, and fortifying the overall security posture of FL systems are critical considerations. Ongoing research is focused on developing cryptographic techniques and secure aggregation methods to mitigate these security concerns.

c. Non-IID Data

Federated Learning assumes that the data on local devices is independent and identically distributed (IID). However, real-world data often deviates from this idealized assumption, presenting a challenge known as non-IID data. Data on different devices may have varying statistical properties, leading to suboptimal model convergence. Addressing non-IID data is a complex problem that requires the development of algorithms capable of handling diverse and non-uniform datasets, ensuring that the global model accurately represents the knowledge embedded in the decentralized data sources.

d. Communication Overhead

The communication process between local devices and the central server introduces inherent overhead. Transmitting model updates, even in the form of gradients, incurs bandwidth and latency costs. As the number of participating devices increases, so does the potential for communication bottlenecks. Efficient communication protocols are crucial to minimize this overhead and ensure the timely aggregation of model updates. Balancing the need for frequent model updates with the practical constraints of communication resources is a delicate trade-off that researchers and practitioners in FL must navigate.

e. Fault Tolerance

FL systems must contend with the possibility of device failures or dropouts during the training process. Ensuring fault tolerance becomes challenging, especially in scenarios where devices have intermittent connectivity or face hardware issues. Robust mechanisms for handling device failures, rejoining the training process, and maintaining the overall stability of FL systems are essential considerations to enhance the reliability of collaborative model training.

f. Regulatory Compliance

The deployment of Federated Learning systems must adhere to evolving data protection and privacy regulations. Navigating the legal landscape and ensuring compliance with standards such as the General Data Protection Regulation (GDPR) is a challenge. FL systems need to incorporate mechanisms that allow for transparent and auditable data processing, providing assurances to users and regulators about the ethical and lawful handling of personal information.

g. Model Fairness and Bias

Federated Learning introduces challenges related to model fairness and bias. Since training occurs on decentralized datasets, models may inadvertently inherit biases present in local data distributions. Ensuring fairness in predictions and mitigating biases across diverse devices with varying data characteristics is a complex issue that requires careful consideration to avoid perpetuating inequities.