Simpósio de Integração Acadêmica
"Ciências Básicas para o Desenvolvimento Sustentável"
SIA UFV 2023

UFV Universidade Federal de Viçosa

TRANSFERÊNCIA DE APRENDIZADO NO TREINAMENTO DE REDES NEURAIS UTILIZANDO FEDERATED LEARNING

Gabriel dos Santos Bezerra*[1], Vitor Barbosa Carlos De Souza*[2] e Marcos Henrique Fonseca Ribeiro*[3]

***Departamento de Informática / UFV - [1]gabriel.s.bezerra@ufv.br, [2]vitor.souza@ufv.br e [3]marcosh.ribeiro@ufv.br**

Grande Área: Ciências Exatas e Tecnológicas - Área temática: Ciência da computação - Categoria do Trabalho: Pesquisa

Palavras-Chave: Federated Learning, Privacidade de Dados, Redes Neurais

Introdução

O crescimento exponencial da coleta de dados em dispositivos isolados, como smartphones, dispositivos IoT e outras plataformas, em conjunto com o acelerado desenvolvimento de técnicas avançadas de aprendizado de máquina e de Redes Neurais têm apresentado, como um desafio, a tarefa de reunir dados em um único local centralizado, a fim de treinar tais modelos. Além das dificuldades técnicas, a privacidade dos usuários também se torna uma preocupação crucial. Os dados pessoais sensíveis armazenados nesses dispositivos precisam ser protegidos e não podem ser compartilhados indiscriminadamente. A privacidade e a segurança dos dados são aspectos fundamentais para a adoção de qualquer abordagem de aprendizado de máquina em um contexto onde os dados estão armazenados de forma distribuída. Nesse cenário, a estratégia conhecida como *Federated Learning* (FL) tem surgido como uma solução promissora, este paradigma de aprendizado aborda o desafio de treinar modelos de aprendizado de máquina em dispositivos distribuídos sem a necessidade de transferir os dados para um servidor centralizado. Ao invés disso, apenas os parâmetros atualizados do modelo são compartilhados, preservando a privacidade dos usuários.

Objetivos

Investigar e analisar diferentes arquiteturas de comunicação e estratégias de agregação de parâmetros no contexto do *Federated Learning* fazendo um levantamento de características que devem ser consideradas ao se pensar na modelagem de um problema de FL, que, em um próximo trabalho, servirá como referência e ponto de partida para a proposta de uma nova abordagem, que visa reunir os pontos fortes observados nas arquiteturas de comunicação e métodos de agregação analisados.

Material e Método

Para podermos analisar e comparar o desempenho das técnicas de FL precisamos realizar testes e observar o desempenho de cada técnica na solução de um problema. A base de dados escolhida para o estudo foi a "*Dataset Letter Recognition*" empregada na classificação multiclasse de caracteres do alfabeto de acordo com um conjunto de características extraída de imagens dos mesmos.

Para realizar os experimentos foi separada uma fração da base para testar a qualidade do modelo global obtido pela federação e o restante dos dados foi dividido em 13, 26 e 52 conjuntos de dados. Esse conjuntos foram criados de forma a não terem o mesmo tamanho e nem seguir a mesma distribuição de classes, para simular a heterogeneidade estatística comum a um cenário de aprendizado distribuído.

Com as bases locais preparadas simulando os dados reais (*Non IID-Data*), foram implementados os algoritmos de FL com as arquiteturas Cliente-Servidor (C-S) [Figura 1] e *Peer-to-Peer* [Figura 2]. Para a primeira abordagem, duas estratégias de agregação foram testadas, uma onde todos os clientes têm a mesma influência na hora de criar o modelo global (média simples) e outra onde os clientes que possuem mais dados nas suas bases locais têm mais influência (média ponderada). Para a outra arquitetura, há um rodízio de transferência de aprendizado, onde um cliente seleciona aleatoriamente outro para continuar o seu treinamento até que todos os clientes participem do processo.

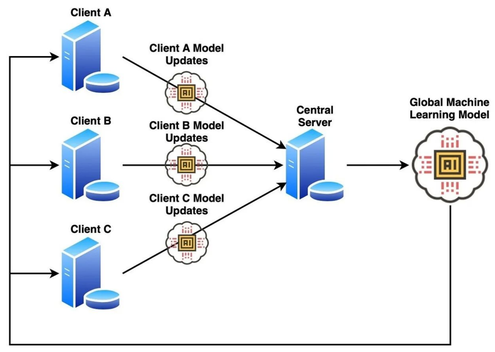

Figura 1: Cliente- Servidor

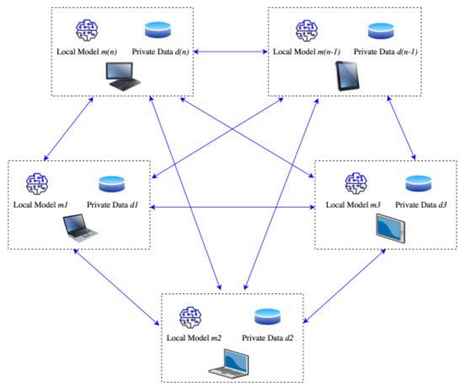

Figura 2: *Peer-to-Peer*

Resultados e Discussão

Foi executado um treinamento não federado, sobre todos os dados para servir como referência e obtivemos uma acurácia de 97.1%. A tabela abaixo traz a comparação dos resultados de acurácia das arquiteturas e os métodos de agregação citados, sobre cada subdivisão de dados:

Arquiteturas / Agregação	N = 13	N = 26	N = 52
C-S Media Simples	91.4%	86.4%	79.5%
C-S Media Ponderada	92.5%	88.4%	81.5%
Peer-to-Peer	94.4%	94.3%	93.4%

Conclusões

O esquema *Peer-to-Peer* mostra resultados melhores que o Cliente-Servidor. A agregação por média ponderada foi ligeiramente melhor que que a por média simples, o que sugere que informações locais a cada nó podem ser úteis para o modelo global. Também pode ser notado que a quantidade de dados por nó é um fator importante (`Tamanho(Base)/N`).

Bibliografia

- Yang, Qiang, et al. "Han Yu. Federated learning." Synthesis Lectures on Artificial Intelligence and Machine Learning 13.3 (2019)
- Li, Tian, et al. "Federated learning: Challenges, methods, and future directions." IEEE signal processing magazine 37.3 (2020): 50-60.