Uma arquitetura escalável e segura para a execução de aprendizado federado no contexto de hospitais inteligentes

Lucas Micol Policarpo[1], **Lucas Mayer Ceschini**[1],
Vinicius Facco Rodrigues[1], **Rodrigo da Rosa Righi**[1]

[1]PPG em Computação Aplicada - Univ. do Vale dos Sinos - São Leopoldo / RS - Brasil

lmpolicarpo@unisinos.br,ceschini.lucas@gmail.com
{vfrodrigues,rrrighi}@unisinos.br

Resumo. *A técnica de aprendizado federado é muito utilizada quando os dados a serem usados pelos modelos de aprendizado de máquina são sensíveis ou sigilosos. No entanto, aprendizado federado prevê o treinamento dos modelos por conta do usuário, que nem sempre está disponível para treinar o modelo ou não possui recursos computacionais eficientes. Esse trabalho apresenta uma arquitetura para execução de aprendizado federado de maneira segura e eficiente utilizando os recursos de borda em hospitais inteligentes.*

1. Introdução

Aprendizado federado, ou *Federated Learning* (FL), é um método de execução de aprendizado de máquina colaborativo, onde várias máquinas treinam várias vezes o mesmo algoritmo com base em amostras de dados locais e apenas os modelos retreinados são compartilhados [Yang et al. 2019]. Essa técnica possibilita o compartilhamento de aprendizado entre os modelos sem a necessidade de troca de dados pela rede. A técnica se mostrou efetiva na pandemia para o diagnóstico de Coronavírus (COVID-19) utilizando modelos compartilhados [Qayyum et al. 2021]. No entanto, existem necessidades computacionais que devem estar disponíveis para a devida execução dos algoritmos. Como o objetivo é manter os dados perto do usuário, quem estiver fazendo uso de FL também fica responsável por treinar aquele algoritmo com base nos próprios dados. Isso normalmente é realizado em uma máquina local que nem sempre está disponível, ou possui os requisitos necessários para uma execução eficiente. Além disso, existem questões de segurança que devem ser endereçadas. Os autores Zhu et al. [Zhu and Han 2020] apresentam um método de ataque de gradiente, onde os dados usados para treinamento podem ser reconstruídos com o modelo treinado. Com isso, a segurança dos dados prevista pelo FL é invalidada.

Tendo em vista os pontos levantados, esse trabalho apresenta um modelo para a execução de FL de maneira eficiente e segura. No caso, fazemos uso de criptografia homomórfica na arquitetura, visando proteger os dados dos usuários mesmo com o compartilhamento dos gradientes. Além disso, é proposta uma arquitetura escalável para execução das funções de FL tendo em vista o tópico de hospitais inteligentes. A arquitetura tem como objetivo rodar as requisições de treinamento nas máquinas do hospital de maneira eficiente, liberando a carga do dispositivo móvel do usuário, assim os dados do usuário são processados na borda pelas máquinas locais e não pelo aparelho.

2. Arquitetura proposta

A proposta é um framework para a execução de serviços FL com o objetivo de otimizar chamadas de treinamento e execução de funções de serviços. Para atingir esse objetivo,

propomos uma arquitetura computacional que contempla um método de *off-loading* para a execução de sessões de treinamento usando os recursos de computação locais do hospital. Esta arquitetura está ciente dos recursos disponíveis em cada computador e do estado atual da rede. Desta forma, o distribuidor de carga é capaz de selecionar a instância de descarregamento mais adequada para a execução da chamada de treinamento. Assim, o sistema libera o dispositivo do usuário da execução do treinamento e consegue entregar o carregamento na melhor instância disponível. Isso garante um menor tempo de execução com um modelo de aprendizagem mais rápido devido aos treinamentos contínuos.

A Figura 1 apresenta uma visão geral da arquitetura, onde o nível mais baixo é o dispositivo do usuário. Os dados são coletados e utilizados pelo algoritmo de FL de interesse. Uma vez que uma chamada de treinamento for executada, os dados saem do dispositivo após serem criptografados utilizando criptografia homomórfica e são entregues ao distribuidor de carga. Então, o distribuidor de carga seleciona e aloca uma máquina na rede local para a tarefa de treinamento, que processa o pedido e retorna tanto o modelo retreinado para o usuário assim como envia os gradientes do treinamento ao agregador local do hospital. Esse ciclo se repete toda vez que novos usuários entram na rede do hospital e fazem uso dos algoritmos de FL disponíveis, ou até a convergência do modelo. Os hospitais também podem compartilhar entre si os gradientes dos seus treinamentos locais.

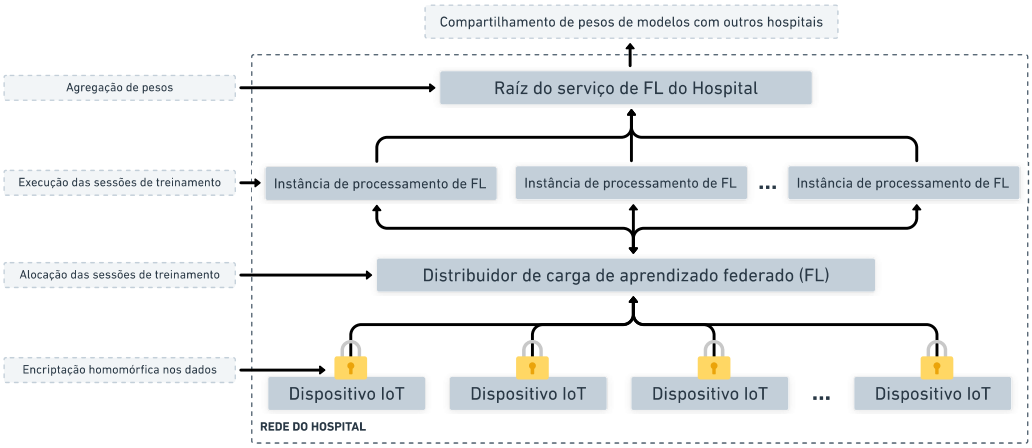

Figura 1. Arquitetura proposta.

Referências

Qayyum, A., Ahmad, K., Ahsan, M. A., Al-Fuqaha, A., and Qadir, J. (2021). Collaborative federated learning for healthcare: Multi-modal covid-19 diagnosis at the edge. *arXiv preprint arXiv:2101.07511*.

Yang, Q., Liu, Y., Cheng, Y., Kang, Y., Chen, T., and Yu, H. (2019). Federated learning. *Synthesis Lectures on Artificial Intelligence and Machine Learning*, 13(3):1–207.

Zhu, L. and Han, S. (2020). Deep leakage from gradients. In *Federated learning*, pages 17–31. Springer.