UNIVERSIDADE FEDERAL DE GOIÁS / INSTITUTO DE INFORMÁTICA

Aprendizado Federado

Compressão de Gradientes Adaptativos em Dados Heterogêneos

Francieli Moreira de Carvalho

UFG
UNIVERSIDADE
FEDERAL DE GOIÁS

UNIVERSIDADE FEDERAL DE GOIÁS (UFG)
INSTITUTO DE INFORMÁTICA (INF)

FRANCIELI MOREIRA DE CARVALHO

Aprendizado Federado

Compressão de Gradientes Adaptativos em Dados Heterogêneos

Goiânia
2025

UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE INFORMÁTICA

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TRABALHO DE CONCLUSÃO DE CURSO DE GRADUAÇÃO NO REPOSITÓRIO INSTITUCIONAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio do Repositório Institucional (RI/UFG), regulamentado pela Resolução CEPEC no 1240/2014, sem ressarcimento dos direitos autorais, de acordo com a Lei no 9.610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou download, a título de divulgação da produção científica brasileira, a partir desta data.

O conteúdo dos Trabalhos de Conclusão dos Cursos de Graduação disponibilizado no RI/UFG é de responsabilidade exclusiva dos autores. Ao encaminhar(em) o produto final, o(s) autor(a)(es)(as) e o(a) orientador(a) firmam o compromisso de que o trabalho não contém nenhuma violação de quaisquer direitos autorais ou outro direito de terceiros.

1. Identificação do Trabalho de Conclusão de Curso de Graduação (TCCG)

Nome(s) completo(s) do(a)(s) autor(a)(es)(as): FRANCIELI MOREIRA DE CARVALHO

Título do trabalho: Aprendizado Federado

Compressão de Gradientes Adaptativos em Dados Heterogêneos

2. Informações de acesso ao documento (este campo deve ser preenchido pelo orientador) Concorda com a liberação total do documento [X] SIM [ ] NÃO[1]

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. Após esse período, a possível disponibilização ocorrerá apenas mediante: a) consulta ao(à)(s) autor(a)(es)(as) e ao(à) orientador(a); b) novo Termo de Ciência e de Autorização (TECA) assinado e inserido no arquivo do TCCG. O documento não será disponibilizado durante o período de embargo.

Casos de embargo:

- Solicitação de registro de patente;

- Submissão de artigo em revista científica;

- Publicação como capítulo de livro.

Obs.: Este termo deve ser assinado no SEI pelo orientador e pelo autor.

Documento assinado eletronicamente por **Francieli Moreira De Carvalho**, **Discente**, em 11/01/2025, às 14:29, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Fernando Marques Federson**, **Professor do Magistério Superior**, em 15/01/2025, às 16:14, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5089567** e o código CRC **A7AA6505**.

Referência: Processo nº 23070.001558/2025-41 SEI nº 5089567

FRANCIELI MOREIRA DE CARVALHO

Aprendizado Federado

Compressão de Gradientes Adaptativos em Dados Heterogêneos

Relatório final de Trabalho de Conclusão de Curso, apresentado à Universidade Federal de Goiás, como parte das exigências para a obtenção do título de Bacharel em Inteligência Artificial.
Orientador: Prof. Dr. Fernando Marques Federson

Goiânia
2025

Ficha de identificação da obra elaborada pelo autor, através do
Programa de Geração Automática do Sistema de Bibliotecas da UFG.

CARVALHO, FRANCIELI MOREIRA DE
Aprendizado Federado [manuscrito] : Compressão de Gradientes Adaptativos em Dados Heterogêneos / FRANCIELI MOREIRA DE CARVALHO. - 2025.
55 f.

Orientador: Prof. Dr. Fernando Marques Federson.
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Goiás, Instituto de Informática (INF), Inteligência Artificial, Goiânia, 2025.

1. inteligência artificial. 2. aprendizado federado. 3. compressão de gradientes. I. Federson, Fernando Marques , orient. II. Título.

CDU 004

FRANCIELI MOREIRA DE CARVALHO

Aprendizado Federado

Compressão de Gradientes Adaptativos em Dados Heterogêneos

Relatório final de Trabalho de Conclusão de Curso, apresentado à Universidade Federal de Goiás, como parte das exigências para a obtenção do título de Bacharel em Inteligência Artificial.

Data da Aprovação: 17 de dezembro de 2024.

Prof. Dr. Fernando Marques Federson
Orientador (INF-UFG)

Prof. Dr. Aldo André Díaz Salazar
Coordenador de TCC do BIA (INF-UFG)

Prof. Dr. Anderson da Silva Soares
Coordenador do BIA (INF-UFG)

TAE Me. Raimunda Delfino dos Santos Aguiar
(INF-UFG)

FRANCIELI MOREIRA DE CARVALHO

Aprendizado Federado

Compressão de Gradientes Adaptativos em Dados Heterogêneos

RESUMO

Este Relatório de Conclusão de Curso tem como objetivo reunir os resultados da minha jornada para me tornar um especialista em **Aprendizado Federado (Comunicação)**. Uma ilustração e sua narrativa descrevem os períodos de trabalho. Os Apêndices contêm os Termos de Aceite de Entrega e os resultados obtidos durante cada período de trabalho.

Palavras-chave: inteligência artificial, modelos grandes de linguagem, geração automática de datasets.

ABSTRACT

This Course Completion Report aims to bring together the results of my journey to become an expert in **Federated Learning (Communication)**. An illustration and its narrative describe the work periods. The Appendices contain the Delivery Acceptance Terms and the results obtained during each work period.

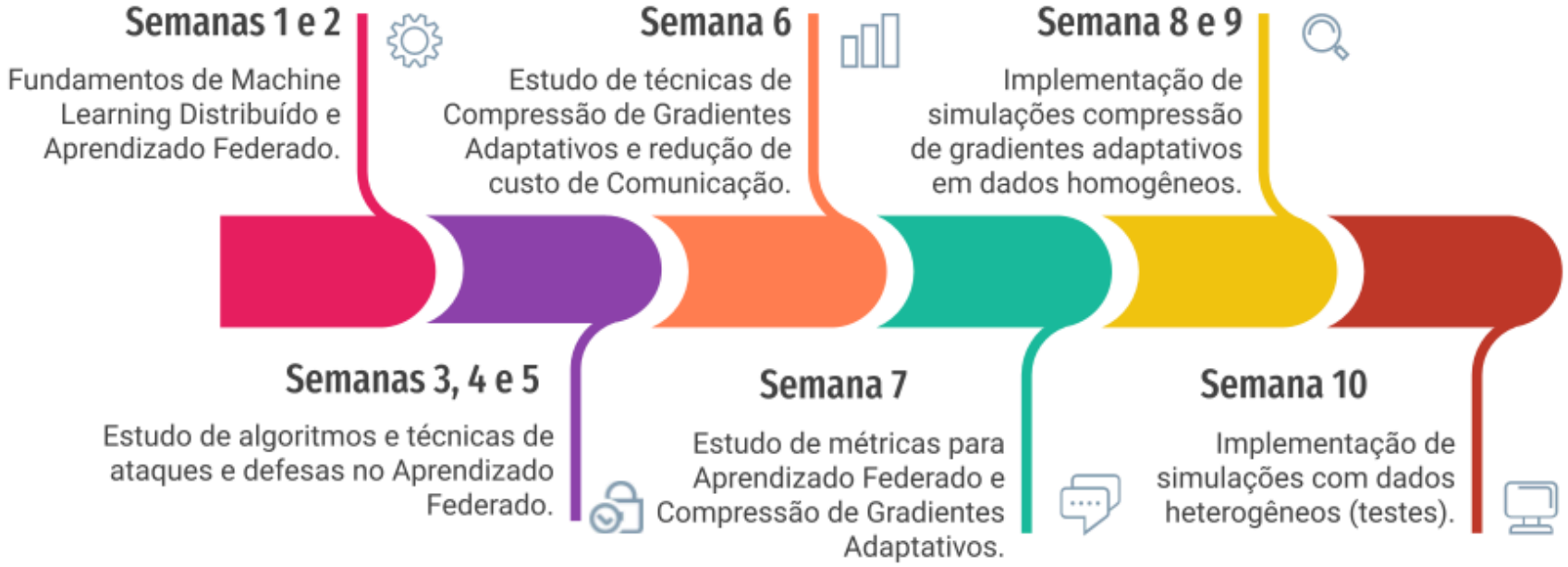
Keywords: artificial intelligence, large language models, automatic dataset generation.

Goiânia

2025

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE INFORMÁTICA

Minha Jornada



Francieli Moreira de Carvalho
Especialista em: Aprendizado Federado (Comunicação)

MINHA JORNADA

Nome: **Francieli Moreira de Carvalho**

Especialidade: **Aprendizado Federado (Comunicação)**

Objetivo deste documento

Durante o processo da disciplina Residência em IA[1], foram gerados diversos resultados na construção da minha especialização. A cada semana, um conjunto de resultados foi formalizado por um Termo de Aceite de Entrega e avaliado por uma banca, considerando o planejado e o realizado para o período. Este documento tem como objetivo descrever esses resultados obtidos, fazendo referência aos Termos de Aceite de Entrega e seus documentos associados.

Minha Jornada

Minha Jornada começou na **Semana 1**, tendo como referência o *Congress in Computer Science, Computer Engineering, and Applied Computing (CSCE 2024)* e minhas vivências durante o Bacharelado em Inteligência Artificial. Foi nesse período que defini a área de conhecimento na qual gostaria de me especializar. A escolha pelo tema Aprendizado Federado foi motivada pelo desejo de sair da zona de conforto, enfrentar novos desafios intelectuais e práticos. O Aprendizado Federado não apenas exige uma compreensão profunda de algoritmos de aprendizado, mas também de como integrar esses algoritmos a infraestruturas distribuídas, enfrentar limitações de comunicação e lidar com a heterogeneidade dos dispositivos, especialmente no contexto de dispositivos IoT e redes 5G. Para embasar o estudo, foram analisados artigos que foram essenciais para compreender os alicerces dessa área: *A Survey on Distributed Machine Learning*, *From Distributed Machine Learning to Federated Learning: A Survey* e *Federated Learning: Opportunities and Challenges*. Esses trabalhos abordam desde a evolução do aprendizado distribuído até os princípios fundamentais do aprendizado federado, destacando técnicas de

[1] Dez semanas, entre setembro de 2024 e dezembro de 2024.

paralelismo, como paralelismo de dados e modelos, além de cenários de aplicação, como FL Vertical, FL Horizontal e FL Híbrido. Outro ponto central abordado foi a importância da privacidade e segurança, com conceitos como privacidade diferencial, criptografia homomórfica e agregação segura. Mais detalhes sobre a Semana 1 podem ser encontrados no **Apêndice 1**.

Na **Semana 2**, os estudos progrediram com um foco mais específico nos algoritmos de Aprendizado Federado (FL). O objetivo principal foi identificar suas características, vantagens e limitações, especialmente em cenários heterogêneos. Durante esse período, foi elaborado um documento que sintetiza os principais conceitos e descobertas relacionados aos algoritmos investigados. Entre os algoritmos analisados, destacam-se o FedAvg, FedProx, SCAFFOLD, FedNova, q-FedAvg e FedMed. Essa análise permitiu uma melhor compreensão das aplicações práticas desses algoritmos no Aprendizado Federado. O documento citado pode ser encontrado no **Apêndice 2.**

Na **Semana 3**, aprofundei meus estudos sobre as ameaças de segurança no Aprendizado Federado (FL), especialmente no contexto de dispositivos IoT. Durante essa semana, analisei como o FL pode resolver problemas de fragmentação de dados e privacidade ao permitir o treinamento de modelos localmente, sem a necessidade de compartilhar os dados. O foco esteve nas ameaças de vazamento de gradientes e ataques baseados em GANs, além das possíveis soluções de mitigação, como Privacidade Diferencial, Encriptação Homomórfica e Ambientes de Execução Confiáveis (TEEs). Também explorei estratégias para aumentar a eficiência de comunicação, como o uso de compactação de modelos por meio do FedSketch e a seleção de clientes baseada em métricas personalizadas (MetricBasedSelection). Paralelamente, comecei a explorar repositórios de código, verificando se os artigos analisados disponibilizam seus códigos em plataformas como o GitHub, visando facilitar futuras implementações práticas. O documento com esses estudos podem ser encontrados no **Apêndice 3.**

Diante de um questionamento recebido na semana anterior, as **Semanas 4 e 5** foram dedicadas a compreender por que os ataques de gradientes são considerados um problema

específico do Aprendizado Federado e não apenas um problema de rede. Para responder a essa questão, aprofundei minha compreensão sobre a natureza desses ataques e suas implicações no contexto do FL. Realizei uma revisão de artigos que discutem técnicas de defesa, como a adição de ruído, poda de gradientes, privacidade diferencial e criptografia homomórfica. Além disso, explorei diferentes tipos de ataques no FL, destacando categorias como Ataque de Inversão de Gradientes, Ataque de Inferência de Associação e Ataque de Envenenamento de Modelos, entre outros. A revisão desses artigos pode ser encontrada no **Apêndice 4**.

Na **Semana 6**, reavaliei o foco da pesquisa, que inicialmente estava direcionado para segurança no Aprendizado Federado, e decidi explorar mais profundamente a eficiência de comunicação e a otimização de recursos. Essa mudança foi motivada pela relevância dessas áreas em contextos como dispositivos IoT e redes móveis, onde a comunicação rápida e eficiente é crítica. Durante essa semana, estudei artigos sobre técnicas de compressão de gradientes, como quantização, esparsificação, compactação, Top-k Esparsificação, Low-Rank Approximation e Feedback de Erro. Um ponto de destaque foi a técnica de Compressão de Gradientes Adaptativa, que ajusta o nível de compressão com base nas condições da rede e dos dispositivos. Além disso, explorei frameworks como TensorFlow Federated, Flower, NS-3 e Omnet++, anotando suas características em uma planilha, mas sem ainda realizar testes aprofundados. As anotações e a planilha citada estão disponíveis no **Apêndice 5**.

Na **Semana 7**, dediquei meus estudos às variáveis e os fatores que impactam a Compressão de Gradientes no contexto do Aprendizado Federado, com um foco particular em dispositivos conectados via redes 5G. Esse aprofundamento buscou entender como as condições de conectividade e as limitações dos dispositivos influenciam diretamente a eficiência e a eficácia das técnicas de compressão aplicadas. Também explorei métricas de avaliação usadas para analisar a eficiência dos métodos de compressão, destacando a importância de métricas como o tempo de convergência. Outro ponto significativo foi o estudo de um tutorial de Aprendizado Federado utilizando Flower e TensorFlow. Durante essa atividade, explorei o funcionamento do aprendizado federado, desde a divisão de

dados até a configuração de clientes e a avaliação do modelo. No experimento prático, uma rede neural convolucional simples foi treinada para classificar o dataset MNIST em um ambiente federado, onde o servidor central combina os pesos dos modelos treinados localmente em cada cliente, garantindo a privacidade dos dados enquanto promove a eficiência colaborativa. Esses estudos podem ser encontrados no **Apêndice 6**.

Após realizar o estudo do tutorial utilizando Flower e TensorFlow, as **Semanas 8 e 9** foram dedicadas à realização de simulações experimentais com diferentes configurações de Aprendizado Federado, avaliando o impacto da compressão de gradientes sobre a eficiência de comunicação e a precisão dos modelos. Durante esse período, identifiquei que o framework Flower não oferece suporte nativo para compressão de gradientes adaptativa, o que trouxe limitações para a implementação prática dessa técnica. Para superar essa limitação, implementei manualmente a compressão de gradientes adaptativa e integrei essa funcionalidade ao Flower, permitindo uma análise dessa abordagem no contexto do Aprendizado Federado. Os testes incluíram três configurações principais: Aprendizado Federado sem compressão, com compressão de gradientes básica e com compressão de gradientes adaptativa. Todos os experimentos foram realizados em dados homogêneos utilizando o dataset MNIST, uma rede neural simples como modelo base e a estratégia FedAvg, com os dados divididos uniformemente entre 10 clientes ao longo de 5 rodadas de treinamento. Os resultados demonstraram que, sem compressão, o aprendizado foi consistente entre os clientes, mas o tráfego de gradientes foi elevado, indicando baixa eficiência de comunicação. Com a compressão de gradientes básica, houve uma significativa redução no tempo de comunicação entre os clientes e o servidor, embora com pequenas perdas de precisão. A compressão adaptativa, por sua vez, preservou melhor as informações importantes nos gradientes, mas apresentou um leve aumento no tempo de execução em relação à compressão fixa. Um Relatório com as simulações realizadas pode ser encontrado no **Apêndice 7**.

Na **Semana 10**, as simulações foram uma extensão das análises anteriores, agora considerando distribuições de dados não-IID entre os clientes simulados, visando aproximar as condições mais próximas de aplicações reais no contexto do Aprendizado Federado. Os

datasets utilizados nas simulações foram o MNIST e o CIFAR-10, com os dados distribuídos de forma heterogênea entre 10 clientes simulados. A técnica de agregação aplicada continuou sendo a estratégia FedAvg, responsável por combinar os gradientes dos modelos locais. Para o modelo, utilizou-se uma Rede Neural Convolucional Simples (CNN) composta por camadas convolucionais e densas, que foi treinada em cada cliente e agregada no servidor central. Os datasets experimentais e modelos simples foram escolhidos para reduzir a complexidade do experimento e focar na avaliação da técnica de compressão adaptativa. Os resultados demonstraram que a Compressão de Gradientes Adaptativa melhora significativamente a eficiência de comunicação, reduzindo o volume de dados transmitidos entre os clientes e o servidor, enquanto preserva uma precisão satisfatória nos modelos. Essa técnica revelou-se especialmente promissora em cenários com dados heterogêneos, destacando-se como uma solução eficiente que equilibra comunicação e desempenho, e abre caminho para futuras otimizações e aplicações práticas no Aprendizado Federado. Mais detalhes são encontrados no **Apêndice 8**.

Essas dez Semanas da Residência foram um grande aprendizado. Desde o início, com os estudos teóricos, até os testes práticos, passei por desafios que me impulsionaram a crescer não apenas tecnicamente, mas também como pesquisadora. Foi um período de muito trabalho, descobertas e resiliência, onde enfrentei limitações práticas, como a implementação manual de soluções adaptativas, além de investigar o impacto do Aprendizado Federado em cenários distribuídos. A mudança de dados homogêneos para heterogêneos foi desafiadora, evidenciando a complexidade e as nuances dessa área. Cada pequena conquista trouxe um sentimento de realização e reforçou minha confiança de que estava trilhando o caminho certo para me tornar uma especialista em Aprendizado Federado. Mais do que aprender técnicas específicas, a residência me mostrou que, com dedicação, posso alcançar ótimos resultados em qualquer área que eu escolher me aprofundar.

APÊNDICE 1

Termo de Aceite de Entrega

Objetivo deste documento

Este documento faz parte do Processo da disciplina Residência em IA e tem como objetivo formalizar o aceite da entrega considerando o planejado e o realizado para o período.

Data da Reunião ("gate") de aprovação: 18 de set. de 2024

Participantes da Entrega [matriculados em Residência em IA]:

Francieli Moreira de Carvalho

Entrega: [descrever a ENTREGA: requisitos e produtos gerados: links para textos, códigos, vídeos etc.]

Para o Gate 1, dediquei os estudos ao entendimento inicial do tema **Aprendizado Federado**, focando em **como a tecnologia surgiu**, seus **principais fundamentos** e a existência de algumas **ferramentas**. Realizei a leitura de três artigos: *A Survey on Distributed Machine Learning*, *From Distributed Machine Learning to Federated Learning: A Survey* e *Federated Learning: Opportunities and Challenges*, que forneceram uma base para o tema.

Principais aprendizados:

- **Técnicas de Paralelismo**: Paralelismo de dados, Paralelismo de modelos e paralelismo de pipeline.
- **Segurança e privacidade:** Privacidade diferencial, criptografia homomórfica e agregação segura.
- **Cenário de dados:** FL Vertical, VL Horizontal e FL Híbrido.
- **Desafios:** heterogeneidade dos dispositivos, identicamente distribuídos (não-IID e comunicação.
- **Ferramentas:** TensorFlow Federated (TFF) e PySyft.

Artigos e resumo: Estudos de Aprendizado Federado

Planejamento: [descrever o que pretende fazer para realizar a próxima ENTREGA]

- Explorar algoritmos como **FedAvg**, **FedProx**, **FedSGD**, **FedNova**, entre outros, que são usados para melhorar a eficiência, escalabilidade e lidar com privacidade e segurança no FL.

- Conhecer as soluções da literatura que abordam os desafios do Aprendizado Federado (FL), como a **heterogeneidade dos dispositivo**s, dados não-IID e **gargalos de comunicação**.

Observação: [caso precise fazer alguma observação, de qualquer "natureza"]

ACEITE DA ENTREGA:

CEDRIC LUIZ DE CARVALHO: Go!

[Documento citado no Termo de Aceite de Entrega de 18 de setembro]

1. Aprendizado de Máquina Distribuído DML para o Aprendizado Federado (FL)

O aprendizado de máquina distribuído surgiu como uma solução para lidar com o aumento exponencial de dados e a complexidade dos modelos de machine learning. À medida que a quantidade de dados aumentava e os modelos se tornavam mais complexos, tornou-se inviável processar tudo em uma única máquina. Assim, o aprendizado distribuído foi introduzido para dividir o treinamento de modelos entre várias máquinas ou servidores. Isso permitiu que grandes volumes de dados fossem processados em paralelo, aumentando a eficiência e escalabilidade.

Esse movimento foi impulsionado pelos avanços em **computação de alto desempenho (HPC)** e pela disponibilidade de GPUs e TPUs que aceleraram o treinamento de redes neurais. O aprendizado de máquina distribuído tornou-se uma prática padrão para grandes empresas de tecnologia como, Google, Amazon e Microsoft que precisavam treinar modelos de machine learning em escala global.

Em 2016, o aprendizado federado foi introduzido por **Brendan McMahan**, um pesquisador do Google, como uma **extensão do aprendizado de máquina distribuído**, como parte de uma solução para **evitar o envio de dados sensíveis para servidores centrais**, o que representa um grande risco em termos de **segurança e privacidade**. Embora o aprendizado distribuído já resolvesse o problema de escalabilidade, ele ainda exigia que os dados fossem centralizados em servidores. Isso era problemático para indústrias sensíveis, como saúde e telecomunicações, onde o compartilhamento de dados pode violar leis de privacidade.

O contexto inicial que motivou o desenvolvimento do FL foi o crescimento do uso de dispositivos móveis e a coleta massiva de dados pessoais, que, quando centralizados, levantavam preocupações quanto à privacidade. Além disso, o surgimento de leis de proteção de dados, como o **GDPR** na Europa, e regulamentos semelhantes em outras regiões, pressionou a indústria de tecnologia a encontrar soluções que pudessem cumprir esses requisitos legais, sem sacrificar o potencial de aprendizado dos modelos de machine learning.

Em vez de transferir os dados para um servidor central, a abordagem do FL permite que os dados permaneçam localmente nos dispositivos dos usuários, como smartphones, tablets e dispositivos IoT. O treinamento é feito nesses dispositivos locais, e apenas as atualizações dos parâmetros do modelo (não os dados) são enviados para um servidor central, onde essas atualizações são combinadas para criar um modelo global. O FL expandiu o aprendizado distribuído, aplicando-o a ambientes onde a privacidade é uma preocupação primordial.

2. Fundamentos do Aprendizado Federado (FL)

O ciclo de vida do modelo federado começa com a criação de um modelo global, que é distribuído para dispositivos locais, como smartphones ou outros dispositivos IoT. Cada dispositivo usa seus dados locais para treinar o modelo e, em vez de enviar os dados para o servidor central, compartilha apenas as atualizações dos parâmetros do modelo. O servidor central, então, agrega essas atualizações, utilizando algoritmos como o **FedAvg**, que calcula uma média ponderada das contribuições dos dispositivos. O modelo global atualizado é redistribuído aos dispositivos, e esse processo continua iterativamente até que o modelo atinja a performance desejada.

Para lidar com a complexidade de distribuir o treinamento entre diferentes dispositivos, o FL emprega **técnicas de paralelismo**. O **paralelismo de dados** permite que cada dispositivo treine o modelo com seus próprios dados locais, sem precisar compartilhar esses dados. O **paralelismo de modelos** distribui partes diferentes de um modelo complexo entre vários dispositivos, enquanto o **paralelismo em pipeline** permite que diferentes camadas de uma rede neural sejam treinadas sequencialmente em dispositivos distintos. O **paralelismo híbrido** combina essas abordagens, ajustando-se à capacidade computacional de cada dispositivo e ao tipo de modelo que está sendo treinado.

Um dos principais pilares do FL é a **segurança e privacidade**. Como os dados nunca saem dos dispositivos locais, técnicas adicionais são aplicadas para garantir que mesmo as atualizações de parâmetros não revelem informações sensíveis. A **privacidade diferencial** adiciona ruído às atualizações, tornando impossível inferir dados individuais dos usuários a partir dos parâmetros compartilhados. A **criptografia homomórfica** permite que os dados permaneçam criptografados durante o treinamento, protegendo as informações mesmo

quando processadas. Além disso, a **agregação segura** impede que o servidor central veja as atualizações individuais de cada dispositivo, garantindo que os dados pessoais não sejam expostos.

O FL também se adapta a diferentes **cenários de dados**, o que amplia suas aplicações. No **FL horizontal**, os dispositivos têm tipos de dados semelhantes, como smartphones de diferentes usuários treinando um modelo de previsão de texto. No **FL vertical**, os dispositivos compartilham dados complementares sobre os mesmos usuários, como uma instituição financeira e um hospital que colaboram para treinar um modelo sem compartilhar diretamente os dados completos de seus clientes. O **FL híbrido** combina aspectos de ambos os cenários, dependendo das necessidades específicas do sistema e da natureza dos dados.

No entanto, o FL enfrenta desafios importantes. A **heterogeneidade dos dispositivos** é um dos maiores obstáculos, já que diferentes dispositivos têm capacidades computacionais e conectividades variadas, o que pode impactar a eficiência do treinamento. Além disso, os dados nos dispositivos podem não ser **identicamente distribuídos (não-IID)**, o que significa que os dados locais de um dispositivo podem ser muito diferentes dos de outros dispositivos. Isso pode dificultar a criação de um modelo global que funcione bem para todos. Outro desafio é a **comunicação** entre os dispositivos e o servidor central, que pode ser um gargalo quando há muitos dispositivos participando do treinamento.

3. Ferramentas

Entre as principais ferramentas de Aprendizado Federado estão:

- **TensorFlow Federated (TFF):** Extensão do TensorFlow, desenvolvido pelo Google, que facilita a simulação e implementação de FL, amplamente utilizado para pesquisas e aplicações em dispositivos móveis.
- **PySyft:** Criado pelo OpenMined, é uma biblioteca de código aberto que possibilita FL com suporte a privacidade diferencial e criptografia homomórfica, ideal para ambientes onde a segurança de dados é crítica, como na saúde.
- PaddleFL: Parte do PaddlePaddle, desenvolvido pela Baidu, oferece suporte a cenários de FL horizontal e vertical, sendo usado em aplicações empresariais de larga escala.
- FATE (Federated AI Technology Enabler): Desenvolvido pela Webank, suporta FL em larga escala com uma variedade de algoritmos de machine learning e preservação de privacidade, usado principalmente em saúde e finanças.
- Leaf: Focado em benchmarks para FL, permite a avaliação de algoritmos em ambientes com alta heterogeneidade de dispositivos e dados não balanceados.

- **OpenFL:** Desenvolvido pela Intel, é uma plataforma de código aberto voltada para o setor de saúde, permitindo treinamento colaborativo sem violar a privacidade dos dados dos pacientes.
- Nvidia Flare: É mantida pela equipe da NVIDIA, com foco em segurança e governança. Ele oferece uma vasta gama de recursos bem projetados, incluindo preservação de privacidade (com privacidade diferencial e criptografia homomórfica) e uma arquitetura reforçada por segurança. FLARE facilita o uso de plataformas como **MONAI** e **Hugging Face**, permitindo a integração com fluxos de trabalho de machine learning existentes, como **PyTorch**, **RAPIDS**, **NeMo** e **TensorFlow**.

Referências:

Artigo	Autores e Ano	Objeto de Estudo	Métricas do objeto
A Survey on Distributed Machine Learning	Joost Verbraeken, Matthijs Wolting, Jonathan Katzy, Jeroen Kloppenburg, Tim Verbelen, Jan S. Rellermeyer	Estudo sobre **aprendizado de máquina distribuído (DML)** e como lidar com grandes volumes de dados.	**Eficiência de comunicação**, **tempo de processamento**, **escalabilidade**, **uso eficiente de recursos computacionais**, e **equilíbrio entre divisão de dados e modelos**.
From Distributed Machine Learning to Federated Learning: A Survey	Qiang Yang, Yang Liu, Tianjian Chen, Yongxin Tong	Explora a **evolução do aprendizado de máquina distribuído (DML) para o aprendizado federado (FL)**, com foco em como o FL resolve **desafios de privacidade e segurança**, mantendo os **dados nos dispositivos locais e compartilhando apenas atualizações de modelos.**	**Preservação da privacidade**, **eficiência de comunicação** (FedAvg), **heterogeneidade dos dispositivos**, **distribuição de dados não-idênticos (não-IID)**, e **escalabilidade** em diferentes cenários (FL horizontal e vertical).
Federated Learning:	Federated Learning:	Exploração das **oportunidades e**	**Sobrecarga de comunicação, resiliência a ataques**

Opportunities and Challenges	Opportunities and Challenges 2021	**desafios do FL**, com ênfase em **comunicação** e **segurança**.	**(envenenamento de modelos, backdoor), incentivos para participação, e eficiência energética.**

APÊNDICE 2

Termo de Aceite de Entrega

Objetivo deste documento

Este documento faz parte do Processo da disciplina Residência em IA e tem como objetivo formalizar o aceite da entrega considerando o planejado e o realizado para o período.

Data da Reunião ("gate") de aprovação: **25 de set. de 2024**

Participantes da Entrega **[matriculados em Residência em IA]**:

Francieli Moreira de Carvalho

Entrega: **[descrever a ENTREGA: requisitos e produtos gerados: links para textos, códigos, vídeos etc.]**

Para o Gate 2, meus estudos focaram na **exploração dos Algoritmos de Aprendizado Federado (FL)**. O objetivo principal foi identificar os **principais algoritmos** utilizados nessa área e entender em quais **contextos eles são mais eficazes**. Ao longo da análise, procurei não apenas conhecer as características de cada algoritmo, mas também compreender suas **vantagens e limitações**, especialmente em cenários de **dados e dispositivos heterogêneos**.

Durante a investigação, destaquei os seguintes algoritmos, junto com suas principais vantagens e limitações:

1. **FedAvg**: Simples e escalável, mas com desempenho fraco em dados heterogêneos (não-i.i.d.).
2. **FedProx**: Robusto para dados e dispositivos heterogêneos, mas com convergência mais lenta.
3. **SCAFFOLD**: Corrige desvios de clientes, mas tem alto custo computacional.
4. **FedNova**: Estabiliza redes heterogêneas, mas é mais complexo de implementar.
5. **q-FedAvg**: Melhora a equidade entre dispositivos, mas com baixa eficiência de comunicação.
6. **FedMed**: Robusto contra outliers, mas com menor precisão em dados heterogêneos.

Essa abordagem permitiu compreender melhor as **vantagens** e **limitações** de cada algoritmo e como eles são aplicados em cenários diversos, como **heterogeneidade de dados** e **dispositivos**, **privacidade** e **eficiência de comunicação**.

Resumo dos estudos realizados: Estudos de FL_v02

Planilha com anotações dos Artigos: Pesquisa Bibliográfica de FL

Planejamento: [descrever o que pretende fazer para realizar a próxima ENTREGA]

- Investigar mais profundamente as técnicas de **privacidade diferencial e segurança** aplicadas ao FL, como **differential privacy**, **encriptação homomórfica**, e **multi-party computation**.

Observação: [caso precise fazer alguma observação, de qualquer "natureza"]

Dentro do tema Aprendizado Federado acredito que quero direcionar a minha pesquisa para Segurança e Privacidade em FL, porém irei fazer uma pesquisa mais detalhada sobre essa parte para realmente decidir.

ACEITE DA ENTREGA:

LEONARDO ALVES: Go!

[Documento citado no Termo de Aceite de Entrega de 25 de setembro]

Introdução

O **aprendizado federado** está emergindo como uma abordagem inovadora no campo do aprendizado de máquina, permitindo que modelos sejam treinados de maneira distribuída, mantendo os dados localmente nos dispositivos. Isso resolve uma preocupação crescente com a privacidade e segurança dos dados, evitando a necessidade de transferir informações sensíveis para um servidor central.

Este trabalho tem como objetivo explorar o aprendizado federado, investigando os principais conceitos, desafios e potenciais aplicações. A pesquisa está em andamento e visa construir uma visão mais clara sobre como o aprendizado federado pode ser aplicado de forma eficiente, com atenção especial às questões de privacidade, segurança e escalabilidade.

À medida que a pesquisa avança, serão analisadas diferentes abordagens técnicas, frameworks e métodos de agregação que suportam o aprendizado federado. Espera-se que,

ao final do estudo, seja possível mapear as principais contribuições da literatura e identificar lacunas e oportunidades para trabalhos futuros.

2. Fundamentos do Aprendizado Federado

➔ **Artigo 1:A Survey on Distributed Machine Learning (Verbraeken et al., 2020)**

Resumo: Este artigo discute as técnicas de aprendizado de máquina distribuído, comparando-as com o aprendizado centralizado, e introduz conceitos de paralelização de dados e modelos que podem ser aplicados ao aprendizado federado.

- **Contribuições principais:** O artigo fornece uma estrutura para análise e desenvolvimento de sistemas distribuídos.
- **Desafios**: Escalabilidade e custos de comunicação entre os dispositivos.
- **Ferramentas:** TensorFlow, Apache Spark, PyTorch.

➔ **Artigo 2: From Distributed Machine Learning to Federated Learning (Liu et al., 2022)**

Resumo: O artigo oferece uma visão geral sobre a evolução do aprendizado de máquina distribuído para o aprendizado federado, detalhando técnicas de paralelização e algoritmos de agregação.

- **Contribuições principais**: O estudo propõe uma arquitetura funcional para sistemas de aprendizado federado, categorizando os principais frameworks e algoritmos utilizados.
- **Desafios**: Privacidade dos dados e latência na comunicação entre dispositivos são questões fundamentais abordadas.
- **Ferramentas**: TensorFlow Federated, PySyft, FATE.

➔ **Artigo 3: Federated Learning: Opportunities and Challenges (Mammen, 2021)**

Resumo: O artigo explora as oportunidades e desafios do aprendizado federado, discutindo vulnerabilidades de segurança e privacidade, além de aplicações em setores como saúde, finanças e transporte.

- **Contribuições principais**: O artigo identifica as principais vulnerabilidades no aprendizado federado, como envenenamento de modelo e ataques de inferência, e sugere defesas baseadas em privacidade diferencial e computação segura.
- **Desafios**: Comunicação, heterogeneidade dos dispositivos e ameaças de privacidade.
- **Ferramentas**: Google FL, Secure Computation, Differential Privacy.

3. Algoritmos de Aprendizado Federado

3.1 Heterogeneidade de Dados (não-IID) e Heterogeneidade de Dispositivos

➔ **Artigo 4:** Heterogeneous Federated Learning: State-of-the-art and Research Challenges (2023)

Resumo: Este artigo explora como a heterogeneidade dos dados impacta o desempenho e propõe uma classificação de soluções em três níveis: **dados**, **modelos** e **servidor**.

Contribuições principais: Métodos de mitigação, como **distilação de conhecimento** e **data augmentation**, são sugeridos para melhorar a performance do FL com dados não-IID.

➔ **Artigo 5:** On the Performance of Federated Learning Algorithms for IoT (Tahir & Ali, 2022)

Resumo: O artigo analisou o desempenho de diversos algoritmos de aprendizado federado em ambientes de **Internet das Coisas (IoT)**, onde a **heterogeneidade dos dispositivos e dos dados** é uma característica fundamental. A seguir, estão os algoritmos avaliados:

FedAvg (Federated Averaging)

- **Descrição**: Um dos algoritmos mais simples e comuns no aprendizado federado. Ele agrega a média ponderada dos modelos locais treinados nos dispositivos. No entanto, o artigo observou que, em ambientes com alta heterogeneidade de dados (não-IID) e dispositivos, o FedAvg sofre uma queda de precisão de até **7.09%**.
- **Vantagens**: Simplicidade e eficiência em redes homogêneas.
- **Limitações**: Não lida bem com a heterogeneidade de dados e dispositivos, o que leva à degradação do desempenho.

FedProx (Federated Proximal)

- **Descrição**: Uma extensão do FedAvg, que inclui um termo de regularização para lidar com a heterogeneidade de sistemas e dados. Nos experimentos do artigo, o FedProx teve uma performance superior ao FedAvg, com uma queda de precisão de apenas **4.84%** em cenários heterogêneos.
- **Vantagens**: Mais robusto em cenários não-IID e com dispositivos com capacidades variáveis.
- **Limitações**: O aumento do tempo de convergência pode ser uma preocupação em alguns cenários.

FedPD (Federated Primal-Dual)

- **Descrição**: Algoritmo baseado em otimização primal-dual, projetado para melhorar o desempenho em cenários com dados não convexos e heterogêneos. No entanto, o FedPD apresentou uma queda de precisão de **30.24%** em cenários altamente heterogêneos, indicando sua vulnerabilidade em redes IoT.
- **Vantagens**: Pode melhorar a eficiência em redes com dados heterogêneos.
- **Limitações**: O desempenho pode ser comprometido em ambientes com alta variabilidade de dispositivos.

SCAFFOLD (Stochastic Controlled Averaging)

- **Descrição**: Algoritmo que tenta mitigar os efeitos da heterogeneidade usando variáveis de controle que reduzem a variância entre as atualizações locais dos dispositivos. Apesar de ser eficaz em alguns cenários, o SCAFFOLD ainda apresentou uma queda de precisão de **19.22%** em redes IoT heterogêneas.
- **Vantagens**: Reduz a variância nas atualizações locais e melhora a convergência em cenários não-IID.
- **Limitações**: Tem um alto custo computacional, o que pode limitar sua aplicabilidade prática.

FedMed (Federated Median)

- **Descrição**: Focado em robustez contra outliers e falhas bizantinas, o FedMed utiliza a mediana para agregar os modelos locais. Nos experimentos, o FedMed apresentou uma queda de precisão de **26.02%** em ambientes com dados não-IID, sugerindo que sua robustez vem à custa da eficiência.
- **Vantagens**: Alta robustez contra outliers e falhas bizantinas.
- **Limitações**: Menor eficiência estatística e precisão em cenários heterogêneos.

q-FedAvg

- **Descrição**: Uma variante do FedAvg que dá maior peso aos dispositivos com maior perda durante o treinamento. Isso melhora a equidade no desempenho entre os dispositivos. O artigo observou que o q-FedAvg apresentou uma queda de **20.03%** em precisão sob condições de alta heterogeneidade.
- **Vantagens**: Melhor equidade entre os dispositivos, especialmente em cenários com alta variabilidade de dados.
- **Limitações**: Ainda sofre com baixa eficiência de comunicação e desafios relacionados à heterogeneidade.
-

3.2 Segurança e Privacidade

➔ **Artigo 6:** Federated Learning with Differential Privacy: Algorithms and Performance Analysis (Kang Wei et al., 2019)

Resumo: O artigo propõe o **NbAFL**, um framework que adiciona ruídos gaussianos aos parâmetros locais antes da agregação, garantindo a privacidade diferencial. O estudo desenvolve também um limite teórico para o desempenho do aprendizado federado com privacidade diferencial, revelando um equilíbrio entre a proteção da privacidade e a convergência.

- **Contribuições principais**: A introdução de um esquema de privacidade diferencial aplicado ao aprendizado federado, que proporciona **proteção da privacidade** sem prejudicar drasticamente a precisão dos modelos. Além disso, os autores propõem uma estratégia de agendamento chamada **K-random**, que seleciona um subconjunto de clientes para participar do treinamento em cada rodada, maximizando a privacidade e o desempenho.
- **Desafios**: O principal desafio discutido no artigo é o **equilíbrio entre privacidade e desempenho de convergência**. O uso de privacidade diferencial reduz a precisão dos modelos, uma vez que ruídos são introduzidos para garantir a proteção dos dados. Para alcançar uma boa precisão, é necessário sacrificar parte da proteção da privacidade e vice-versa.
- **Ferramentas**: NbAFL (Noising before Aggregation Federated Learning), ruído Gaussiano para privacidade diferencial.

Link da planilha com mais análise dos artigos: Pesquisa Artigos sobre FL

APÊNDICE 3

Termo de Aceite de Entrega

Objetivo deste documento

Este documento faz parte do Processo da disciplina Residência em IA e tem como objetivo formalizar o aceite da entrega considerando o planejado e o realizado para o período.

Data da Reunião ("gate") de aprovação: 3 de out. de 2024

Participantes da Entrega [matriculados em Residência em IA]:

Francieli Moreira de Carvalho

Entrega: [descrever a ENTREGA: requisitos e produtos gerados: links para textos, códigos, vídeos etc.]

Para o gate 03 os principais pontos abordados foram:

- **Aprendizado Federado em IoT**: Analisei como o FL pode resolver problemas de **fragmentação de dados** e **privacidade** ao permitir o treinamento de modelos localmente, sem que os dados precisem ser compartilhados.
- **Ameaças de segurança no FL**:
  - **Vazamento de gradientes**
  - **Ataques baseados em GANs**
- **Soluções de mitigação**:
  - **Privacidade Diferencial**
  - **Encriptação Homomórfica**
  - **Ambientes de Execução Confiáveis (TEEs)**
- **Eficiência de comunicação**:

- **FedSketch**: Compactação de modelos para reduzir custos de comunicação.
- **MetricBasedSelection**: Seleção de clientes com base em métricas personalizadas.

Além disso, comecei a **explorar repositórios de código** para verificar se os artigos analisados disponibilizam seus **códigos em plataformas** como o GitHub, o que pode facilitar a implementação prática das soluções propostas.

Resumo dos estudos realizados: v03 Estudos de FL

Planilha com anotações dos Artigos: Trabalhos_FL

Planejamento: **[descrever o que pretende fazer para realizar a próxima ENTREGA]**

- Verificar **um ou dois repositórios** relacionados aos artigos.
- Baixar e tentar rodar **um exemplo prático** para entender como funciona.

Observação: [caso precise fazer alguma observação, de qualquer "natureza"]

ACEITE DA ENTREGA:

CEDRIC LUIZ DE CARVALHO: Go!

[Documento citado no Termo de Aceite de Entrega de 03 de outubro]

Nessa Etapa busquei entender como o Aprendizado Federado é aplicado a Internet das Coisas (IoT), e também como lidar com os desafios de segurança e privacidade. Durante os estudos, foram analisadas formas de melhorar a comunicação entre os dispositivos, garantir a proteção dos dados e usar os recursos de rede de maneira mais eficiente em sistemas FL

.

➔ **Artigo:** **Aprendizado Federado aplicado à Internet das Coisas**

Resumo: O artigo aborda os fundamentos do **Aprendizado Federado** e como essa tecnologia pode ser uma solução para os desafios de privacidade e fragmentação de dados

na **Internet das Coisas (IoT)**. O **FL** permite o treinamento de modelos de **machine learning** sem que os dados saiam dos dispositivos locais, preservando a privacidade dos usuários.

- ❖ **Contribuições Principais:** Discussão sobre como o **FL** se diferencia do aprendizado de máquina centralizado e descentralizado, com foco nas aplicações de **IoT**, Exploração dos desafios tecnológicos para a implantação de FL, como a compressão de modelos para dispositivos com recursos limitados e Apresentação das principais metodologias e pesquisas existentes no campo do FL aplicadas a **IoT**.
- ❖ Desafios: **Privacidade e segurança dos dados** durante o treinamento federado, **Escalabilidade** e **eficiência de comunicação** entre dispositivos com recursos limitados e **Desempenho** em dispositivos IoT, que possuem limitações de hardware e rede.
- ❖ **Ferramentas**: Não menciona

- **Segurança e Privacidade**

➔ **Artigo:**[Threats, Attacks and Defenses in Federated Learning: Issues, Taxonomy and Perspectives]

Resumo: O artigo explora o panorama atual de ameaças e ataques no contexto do Aprendizado Federado (FL). O FL tem se tornado uma abordagem popular para o aprendizado distribuído, permitindo o treinamento colaborativo de modelos sem centralizar os dados dos usuários. No entanto, essa arquitetura distribuída abre espaço para diversas vulnerabilidades e ameaças à privacidade e à segurança. O artigo categoriza os diferentes tipos de ataques, incluindo **ataques passivos e ativos**, e propõe uma taxonomia detalhada para classificar as ameaças. Além disso, o artigo discute estratégias de defesa, como Privacidade Diferencial, Encriptação Homomórfica e Agregação Segura, e aponta os principais desafios e oportunidades para futuras pesquisas.

- ❖ **Contribuições principais**:A criação de uma **taxonomia detalhada** para classificar ameaças e ataques no FL, diferenciando entre ataques ativos, passivos e localizados no servidor ou nos dispositivos. Além disso, os autores exploram diversas técnicas de **defesa**, incluindo privacidade diferencial e agregação segura, para proteger os dados durante o treinamento distribuído.
- ❖ **Desafios:** O principal desafio discutido é a conciliação entre segurança e desempenho. O uso de técnicas de privacidade e encriptação pode aumentar a segurança, mas afeta a eficiência do treinamento e a convergência dos modelos, especialmente em sistemas distribuídos e heterogêneos.

- **Ferramentas:**Flower Framework, PySyft, e TensorFlow Federated e técnicas como Encriptação Homomórfica e Privacidade Diferencial

➔ **Artigo:** **Security and Privacy Threats to Federated Learning: Issues, Methods, and Challenges**

Resumo: O artigo aborda as ameaças de segurança e privacidade no Aprendizado Federado (FL), classificando diferentes tipos de ataques que podem ocorrer tanto do lado do agregador quanto dos participantes maliciosos. Ele também explora técnicas de mitigação como Privacidade Diferencial, Encriptação Homomórfica e o uso de blockchain e Ambientes de Execução Confiáveis (TEEs) para proteger os dados e o modelo. O artigo destaca a necessidade de maior investigação sobre essas defesas e propõe possíveis direções futuras de pesquisa no campo do FL.

- **Contribuições** Principais: Classifica os ataques no Aprendizado Federado (FL), diferenciando ameaças como vazamento de gradientes e ataques com **GANs**. Ele discute técnicas de mitigação, incluindo **Privacidade Diferencial, Encriptação Homomórfica e blockchain** para melhorar a segurança no FL. Além disso, identifica os desafios de **proteção contra ataques internos**, o **equilíbrio entre privacidade e precisão e a escalabilidade** das soluções em cenários reais.
- **Desafios:** Os principais desafios incluem a **proteção contra ataques internos e externos**, o equilíbrio entre **privacidade e desempenho**, e a necessidade de **escalabilidade** das soluções de segurança sem comprometer a eficiência do aprendizado federado.
- **Ferramentas:** Privacidade Diferencial, Encriptação Homomórfica, SMC (Cálculo Multipartidário Seguro), Ambientes de Execução Confiáveis (TEEs) e blockchain.

➔ **Artigo:** **Privacidade do Usuário em Aprendizado Colaborativo: Federated Learning, da Teoria à Prática**

Resumo: O artigo explora as questões de privacidade e segurança no contexto do Aprendizado Federado (FL), apresentando como os dados dos usuários podem ser protegidos enquanto colaboram no treinamento de modelos de aprendizado de máquina. Ele detalha as ameaças à privacidade no FL, incluindo ataques de envenenamento de dados e inversão de modelo, e discute soluções práticas como criptografia homomórfica e Privacidade Diferencial. O artigo também destaca a implementação prática do FL em aplicações reais e sugere áreas de pesquisa futuras.

- **Contribuições Principais:** Classifica as ameaças de privacidade no FL, destacando ataques como **envenenamento de dados** e **inversão de modelo**. Ele também discute as principais técnicas de mitigação, como **Privacidade Diferencial**, **criptografia homomórfica**, e o uso de **FedAvg** para agregar modelos de maneira segura. Além disso, o artigo identifica os desafios de proteger os dados dos usuários sem comprometer o desempenho do modelo, destacando também o impacto de legislações como a **LGPD**.
- **Desafios: Proteção contra ataques maliciosos** dos próprios participantes, a **manutenção da precisão** do modelo enquanto se preserva a privacidade dos dados e a **escalabilidade** das soluções em sistemas reais, como os usados em aplicações de larga escala como o Gboard.
- **Ferramentas: Privacidade Diferencial**, **criptografia homomórfica**, **FedAvg**, e **Ambientes de Execução Confiáveis (TEEs)** para garantir a segurança dos dados em cenários de Aprendizado Federado.

- **Privacidade e Comunicação**

➔ **Artigo:** **Privacidade e Comunicação Eficiente em Aprendizado Federado: Uma Abordagem Utilizando Estruturas de Dados Probabilísticas e Seleção de Clientes**

Resumo: O artigo propõe o **FedSketch**, que aplica **sketches** para melhorar a privacidade e eficiência na comunicação dos modelos em FL, juntamente com **privacidade diferencial**. Além disso, o **MetricBasedSelection** ajuda a escolher clientes com base em métricas para melhorar o desempenho. A abordagem mostrou-se eficaz ao reduzir os custos de comunicação significativamente, com um alto nível de privacidade diferencial ($\epsilon \approx 10-6$).

- **Contribuições Principais:** Proposta do **FedSketch**, que compacta os modelos de redes neurais para reduzir os custos de comunicação, mantendo alta privacidade e Proposta do **MetricBasedSelection**, que seleciona clientes com base em métricas personalizadas, melhorando a eficiência do treinamento.
- **Desafios: Segurança dos dados** durante o treinamento federado e a **redução dos custos de comunicação** sem comprometer a precisão dos modelos.
- Ferramentas: **Privacidade diferencial** para segurança, e um protocolo de comunicação MQTT para a arquitetura de comunicação cliente-servidor. Além disso, a avaliação foi realizada com os datasets **MNIST**, **FAMNIST**, e **CIFAR10**.

Link da planilha com análise dos artigos dessa semana: Artigos analisados.

APÊNDICE 4

Termo de Aceite de Entrega

Objetivo deste documento

Este documento faz parte do Processo da disciplina Residência em IA e tem como objetivo formalizar o aceite da entrega considerando o planejado e o realizado para o período.

Data da Reunião ("gate") de aprovação: 9 de out. de 2024

Participantes da Entrega [matriculados em Residência em IA]:

Francieli Moreira de Carvalho

Entrega: [descrever a ENTREGA: requisitos e produtos gerados: links para textos, códigos, vídeos etc.]

No Gate passado (Gate 03), fui questionada sobre os ataques de gradientes, que eu havia mencionado como uma das principais ameaças no aprendizado federado (FL). O questionamento foi o seguinte: **por que esses ataques são considerados um problema específico do aprendizado federado e não apenas um problema de rede, já que envolvem o compartilhamento dos gradientes, ou seja, os erros dos modelos?**
Diante desse questionamento, percebi que seria mais sensato focar primeiro em consolidar meu entendimento sobre a natureza dos ataques de gradientes e suas implicações no contexto do FL antes de seguir para a parte prática de explorar repositórios e exemplos de código, que era o que eu havia planejado para esta semana (Gate 04).

Para isso testei a utilização da ferramenta researchrabbit.ai para buscar artigos relacionados ao tema ataques de gradientes em FL e dentre os que selecionei realizei a leitura e anotações dos três seguintes:

1. **A Comprehensive Study of Gradient Inversion Attacks in Federated Learning**: Analisa os ataques de inversão de gradientes, destacando como o conhecimento do adversário, como estatísticas de BatchNorm, afeta a eficácia desses ataques. Propõe a adição de ruído e a poda de gradientes como técnicas de defesa.
2. **Evaluating Gradient Inversion Attacks and Defenses in Federated Learning**: Categoriza os ataques de inversão de gradientes e explora defesas como privacidade diferencial e criptografia homomórfica, com foco na proteção de dados em dispositivos IoT com recursos limitados.
3. **Secure and Efficient Federated Learning Schemes for Healthcare Systems**:O uso do FL em sistemas de saúde e dispositivos IoT, propondo técnicas de criptografia e compressão de gradientes para proteger os dados e melhorar a eficiência de comunicação.

Resumo dos estudos realizados: v04 Estudos de FL
Tabela com anotações dos Artigos: Artigos de FL

Planejamento: [descrever o que pretende fazer para realizar a próxima ENTREGA]

- **Analisar as suposições feitas pelos atacantes e seu impacto na eficácia do ataque.**
- **Pesquisar casos práticos de ataques de gradientes para entender seus cenários mais comuns.**

Observação: [caso precise fazer alguma observação, de qualquer "natureza"]

ACEITE DA ENTREGA:

CEDRIC LUIZ DE CARVALHO: Go!

Termo de Aceite de Entrega

Objetivo deste documento

Este documento faz parte do Processo da disciplina Residência em IA e tem como objetivo formalizar o aceite da entrega considerando o planejado e o realizado para o período.

Data da Reunião ("gate") de aprovação: 16 de out. de 2024

Participantes da Entrega [matriculados em Residência em IA]:

Francieli Moreira de Carvalho

Entrega: [descrever a ENTREGA: requisitos e produtos gerados: links para textos, códigos, vídeos etc.]

Para o Gate 6, eu comecei pesquisando os diferentes tipos de ataques que existem até o momento no Aprendizado Federado, realizando uma comparação entre eles. Encontrei até o momento **12 tipos de ataques**, e abaixo cito os 5 mais comuns:

1. **Ataque de Inversão de Gradientes (Gradient Inversion Attack)**
2. **Ataque de Inferência de Associação (Membership Inference Attack)**
3. **Ataque de Envenenamento de Modelos (Model Poisoning Attack)**
4. **Ataque de Reconstrução de Dados (Data Reconstruction Attack)**
5. **Ataque de Inferência de Propriedades (Property Inference Attack)**

Também comecei a me aprofundar e a comparar as principais técnicas de defesa no Aprendizado Federado, assim como suas **vantagens** e **desvantagens**. Até momento encontrei **10 técnicas de defesas**, sendo as 5 principais listadas abaixo:

1. **Privacidade Diferencial (Differential Privacy - DP)**
2. **Criptografia Homomórfica (Homomorphic Encryption - HE)**
3. **Compressão de Gradientes**
4. **Poda de Gradientes (Gradient Pruning - GradPrune)**
5. **Ambientes de Execução Confiáveis (Trusted Execution Environments - TEEs)**

As anotações podem ser encontradas nessa tabela: Estudos FL

Planejamento: [descrever o que pretende fazer para realizar a próxima ENTREGA]

- Explorar como essas **técnicas podem ser combinadas** para equilibrar **privacidade e eficiência** nos modelos de Aprendizado Federado.
- Baixar e tentar rodar **um exemplo prático que aborda segurança e privacidade** para entender como funciona.

Observação: [caso precise fazer alguma observação, de qualquer "natureza"]

ACEITE DA ENTREGA:

CEDRIC LUIZ DE CARVALHO: Go!

[Documentos citados no Termo de Aceite de Entrega de 09 e 16 de outubro]

Nessa semana, busquei entender ataques de inversão de gradientes e suas defesas no contexto do Aprendizado Federado (FL).

➔ **Artigo:** A Comprehensive Study of Gradient Inversion Attacks in Federated Learning

Resumo: O artigo foca na análise detalhada dos ataques de inversão de gradientes, avaliando as técnicas de defesa existentes e explorando suas limitações. O estudo enfatiza como a eficácia desses ataques depende de suposições específicas sobre o conhecimento do adversário, como as estatísticas de BatchNorm e os rótulos privados. O artigo também investiga como diferentes mecanismos de defesa podem ser combinados para equilibrar a proteção da privacidade e a precisão do modelo.

- **Contribuições principais**: Destaca as suposições feitas pelos ataques de inversão de gradientes, como o conhecimento das estatísticas de BatchNorm e dos rótulos privados, e demonstra que enfraquecer essas suposições reduz significativamente a eficácia dos ataques. Ele também avalia três mecanismos de defesa principais: a adição de ruído aos gradientes, a poda de gradientes e técnicas de codificação de entrada, explorando como essas defesas podem ser combinadas para equilibrar a segurança dos dados e a precisão dos modelos. dispositivos IoT, que possuem recursos limitados de processamento e comunicação.
- **Desafios:** Proteger a privacidade dos dados durante os ataques de inversão de gradientes, lidar com as suposições de conhecimento de estatísticas de BatchNorm e rótulos privados, e minimizar a perda de precisão do modelo ao aplicar defesas..
- **Ferramentas:** poda de gradientes (GradPrune), MixUp e Intra-InstaHide

➔ **Artigo:** [Evaluating Gradient Inversion Attacks and Defenses in Federated Learning]

Resumo: O artigo aborda as ameaças de segurança e privacidade no Aprendizado Federado (FL), classificando diferentes tipos de ataques que podem ocorrer tanto do lado do agregador quanto dos participantes maliciosos. Ele também explora técnicas de mitigação como Privacidade Diferencial, Encriptação Homomórfica e o uso de blockchain e Ambientes de Execução Confiáveis (TEEs) para proteger os dados e o modelo. O artigo destaca a necessidade de maior investigação sobre essas defesas e propõe possíveis direções futuras de pesquisa no campo do FL.

- ❖ **Contribuições Principais:** Detalhada dos **ataques de inversão de gradientes**, classificando-os em diferentes tipos e mostrando como cada um pode ser aplicado para extrair informações dos dados de treinamento. Além disso, o estudo propõe técnicas defensivas, como privacidade diferencial, quantização de gradientes e criptografia homomórfica, que podem ajudar a proteger os dados contra ataques. Ele também discute a eficiência dessas técnicas no contexto de dispositivos IoT, que possuem recursos limitados de processamento e comunicação.
- ❖ **Desafios:** Proteger a privacidade e a segurança dos dados contra ataques que exploram os gradientes, manter a eficiência de comunicação e a escalabilidade do FL, e lidar com as limitações de hardware e rede dos dispositivos IoT. A reconstrução precisa de dados a partir de gradientes interceptados é uma preocupação crítica, e as soluções propostas nem sempre conseguem equilibrar a proteção da privacidade com a manutenção da precisão do modelo.
- ❖ **Ferramentas:** Privacidade diferencial, criptografia homomórfica e compressão de gradientes

➔ **Artigo:** [Secure and Efficient Federated Learning Schemes for Healthcare Systems]

Resumo: O artigo aborda os fundamentos do Aprendizado Federado (FL) e como essa tecnologia pode ser uma solução para os desafios de privacidade e fragmentação de dados na Internet das Coisas (IoT). Ele utiliza técnicas de **criptografia e autenticação para proteger as informações durante o treinamento**, além de otimizar a comunicação entre os dispositivos participantes.

- ❖ **Contribuições Principais:** Detalha os desafios para a implementação do FL, especialmente em dispositivos IoT, que possuem recursos limitados de hardware e rede. Propõe técnicas como compressão de gradientes para reduzir a sobrecarga de comunicação e algoritmos de criptografia que minimizam a exposição dos dados

durante o treinamento. Também apresenta uma análise das principais metodologias e pesquisas existentes no campo do FL aplicadas a IoT, discutindo técnicas como criptografia homomórfica e provas de conhecimento zero para aumentar a segurança dos dados.

- Desafios: Privacidade e segurança dos dados durante o treinamento, a escalabilidade e eficiência de comunicação entre dispositivos e o desempenho em dispositivos IoT. Proteger os dados dos usuários contra ataques que possam inferir informações sensíveis a partir das atualizações de modelo é uma preocupação constante. Além disso, o FL enfrenta dificuldades em manter uma comunicação eficiente, principalmente em **redes com limitações de largura de banda**, sendo necessária a implementação de técnicas de compressão de dados para mitigar esse problema. Por fim, os dispositivos IoT geralmente possuem **limitações de hardware e rede**, o que dificulta a execução de modelos complexos, exigindo soluções que adaptem o treinamento de modelos às capacidades desses dispositivos.
- **Ferramentas**: criptografia homomórfica Paillier, prova de conhecimento zero Schnorr e algoritmo de compressão de gradientes

Link da planilha com anotações dos artigos analisados: Artigos analisados

APÊNDICE 5

Termo de Aceite de Entrega

Objetivo deste documento

Este documento faz parte do Processo da disciplina Residência em IA e tem como objetivo formalizar o aceite da entrega considerando o planejado e o realizado para o período.

Data da Reunião ("gate") de aprovação: 31 de out. de 2024

Participantes da Entrega [matriculados em Residência em IA]:

Francieli Moreira de Carvalho

Entrega: [descrever a ENTREGA: requisitos e produtos gerados: links para textos, códigos, vídeos etc.]

Iniciei minha pesquisa com foco em aprendizado distribuído, o que me levou ao Aprendizado Federado. No começo, fiquei em dúvida entre me concentrar em segurança ou eficiência de comunicação. Inicialmente, optei por explorar temas de segurança, como ataques, defesas, privacidade diferencial e proteção de dados.
Após algumas semanas de leitura, percebi que, embora a segurança seja importante no Aprendizado Federado, a eficiência de comunicação e a otimização de recursos são áreas que podem me proporcionar habilidades valiosas, como escalabilidade e adaptabilidade de algoritmos. Essas competências são especialmente relevantes em contextos como dispositivos IoT e redes móveis, onde a necessidade de comunicação rápida é crítica.

Sendo assim, os avanços para esse Gate foram:

1. **Pesquisas:** Estudei diversos artigos relevantes sobre compressão de gradientes e aprendizado federado, organizando as informações em uma planilha. Durante essa revisão, concentrei-me em várias técnicas fundamentais, incluindo:

- **Quantização**: Reduz a precisão dos gradientes, economizando largura de banda.
- **Esparsificação**: Filtra gradientes de menor impacto, enviando apenas os mais significativos.
- **Compactação**: Utiliza algoritmos de codificação para diminuir o tamanho dos dados transmitidos.
- **Top-k Esparsificação**: Envia apenas os k gradientes de maior magnitude.
- **Low-Rank Approximation**: Representa os gradientes de forma mais eficiente.
- **Feedback de Erro**: Ajusta erros introduzidos pela compressão nas rodadas seguintes.

Achei interessante a técnica de **Compressão de Gradientes Adaptativa**, que ajusta o nível de compressão com base nas condições da rede e dos recursos dos dispositivos.

2. **Exploração de Ferramentas:** Pesquisei frameworks como TensorFlow Federated, Flower, NS-3 e Omnet++ e anotei na planilha na aba frameworks, mas ainda não selecionei ou testei de fato as ferramentas.
3. **Estudo de Métricas:** Comecei a investigar métricas de avaliação que podem ser utilizadas, como

consumo de energia, volume de dados transmitidos e latência, mas nada aprofundado apenas conhecendo.

Material:

- ➔ FL_artigos - Planilhas Google
- ➔ Anotações_FL - Documentos Google

Planejamento: [descrever o que pretende fazer para realizar a próxima ENTREGA]

- **Selecionar e Compreender Variáveis:** Identificar e entender as variáveis que influenciam a Compressão de Gradientes Adaptativa, como a qualidade da conexão 5G e o nível de bateria dos dispositivos.
- **Testar Ferramentas:** Realizar testes iniciais com as ferramentas e frameworks selecionados para entender suas funcionalidades e determinar quais são mais adequados para a pesquisa.
- **Continuar Estudando Métricas de Avaliação:** Aprofundar o estudo sobre as métricas que podem ser utilizadas para avaliar o desempenho da compressão de gradientes.
- **Organizar meu referencial de pesquisa**, pois ele está começando a ficar disperso.

Observação: [caso precise fazer alguma observação, de qualquer "natureza"]

ACEITE DA ENTREGA:

CEDRIC LUIZ DE CARVALHO: Go!

[Documentos citados no Termo de Aceite de Entrega de 31 de outubro]

Iniciei minha pesquisa com foco em aprendizado distribuído, o que me levou naturalmente ao aprendizado federado. No começo, fiquei um pouco indecisa entre focar em segurança ou em eficiência de comunicação, duas áreas que me chamaram muito a atenção. Minha primeira escolha foi explorar temas de segurança mais a fundo, estudando ataques e defesas, além de mergulhar em conceitos como privacidade diferencial e proteção de dados.

Depois de algumas semanas de leitura e reflexão, decidi direcionar o foco para **eficiência de comunicação e otimização de recursos**. Eu já tinha uma vontade inicial de

explorar essa área, e, com mais estudos, percebi que ela não só traz aplicações práticas imediatas como também pode servir como base para trabalhar com segurança futuramente.

Foi assim que defini meu tema: **Compressão de Gradientes Adaptativa para Aprendizado Federado**. Esse foco se apoia em técnicas de compressão que ajustam o nível de comunicação conforme as condições de rede e os recursos de cada dispositivo. Esse tipo de pesquisa atende diretamente a uma demanda crescente no mercado, especialmente em setores que dependem de dispositivos IoT e redes móveis, como saúde, cidades inteligentes e veículos autônomos. Em dispositivos como sensores ambientais, câmeras de segurança e dispositivos médicos, por exemplo, é essencial que a comunicação seja rápida e eficiente, consumindo o mínimo possível de energia. Em dispositivos móveis, otimizar a comunicação e o processamento permite que aplicações complexas, como assistentes pessoais e algoritmos de saúde, funcionem de forma contínua, sem drenar a bateria rapidamente e sem depender de conexão constante a servidores.

Acredito que o **aprendizado federado, com foco em compressão de gradientes adaptativa e otimização de recursos**, não só atende a essas demandas reais do mercado, mas também me ajuda a desenvolver habilidades essenciais na área de Inteligência Artificial e Ciência de Dados, como escalabilidade e adaptabilidade de algoritmos. Além disso, também irá me dar uma base sólida me permiti aprofundamentos futuros em temas de segurança e privacidade no aprendizado federado.

Compressão de Gradientes Adaptativa para Aprendizado Federado

O que é a Compressão de Gradientes?

A **compressão de gradientes** é uma técnica que reduz o volume de dados enviados por dispositivos locais ao servidor central em um sistema de aprendizado federado. Os gradientes representam as "atualizações" necessárias para ajustar os parâmetros do modelo com base nos dados de cada dispositivo. Em vez de enviar todos os gradientes gerados pelo modelo local, a compressão reduz o tamanho dos dados transmitidos, mantendo a informação mais relevante e economizando recursos de comunicação e energia.

Para que é utilizada a Compressão de Gradientes?

A compressão de gradientes é usada para reduzir o consumo de largura de banda e otimizar o uso de energia e processamento nos dispositivos participantes do aprendizado federado. Em redes de dispositivos IoT ou em ambientes de 5G, onde a largura de banda pode ser limitada e os dispositivos possuem capacidade limitada de energia e processamento, a compressão de gradientes permite:

1. Economizar Recursos: Dispositivos IoT têm restrições significativas de energia e capacidade de processamento. A compressão de gradientes diminui a quantidade de dados a ser enviada, reduzindo o consumo de bateria e o tempo necessário para o processamento de cada atualização.
2. Melhorar a Escalabilidade: Com menos dados para transmitir e processar, mais dispositivos podem participar do aprendizado federado sem sobrecarregar a rede ou o servidor central.
3. Viabilizar o Aprendizado em Redes Limitadas: A compressão é essencial para viabilizar a troca de dados em redes onde a largura de banda é limitada, como IoT, e em áreas de baixa conectividade, onde os dispositivos podem precisar de uma comunicação mais econômica.

Como pode ser utilizada a Compressão de Gradientes?

No aprendizado federado, a compressão de gradientes pode ser aplicada de várias formas para otimizar o processo de atualização dos modelos, especialmente em dispositivos conectados via redes IoT e 5G:

1. Compressão Fixa: Aplica uma taxa de compressão constante para todos os dispositivos. Por exemplo, ao utilizar uma quantização que reduz todos os gradientes para uma precisão menor. Em cenários onde as condições de rede e energia são estáveis e homogêneas entre dispositivos.
2. Compressão Esparsificada: Filtra gradientes de menor impacto, enviando apenas os mais significativos. É comumente usada para reduzir drasticamente o volume de dados transmitidos. Em redes com largura de banda extremamente limitada e em dispositivos com pouca energia, onde é necessário reduzir o volume de dados ao mínimo.
3. Compressão Adaptativa: Ajusta a compressão de gradientes dinamicamente, com base nas condições da rede (como qualidade do sinal 5G) e na energia disponível no dispositivo IoT. Quando o sinal é fraco ou a bateria está baixa, aplica-se uma compressão mais agressiva; em condições favoráveis, a compressão é reduzida para preservar a precisão. Em ambientes com variabilidade, como redes 5G e IoT, onde a conectividade e a capacidade do dispositivo podem mudar constantemente.
4. Compressão com Quantização: Reduz a precisão dos gradientes (por exemplo, de valores de ponto flutuante para inteiros de menor precisão). Em contextos onde a precisão dos dados transmitidos pode ser sacrificada em prol de uma comunicação mais leve e rápida, sem comprometer muito a qualidade do modelo.

Adaptabilidade em Algoritmos de IA

Adaptabilidade em algoritmos de Inteligência Artificial (IA) significa que os modelos podem se ajustar automaticamente para lidar com diferentes condições e limitações do ambiente em que estão sendo executados. Isso é especialmente importante em sistemas onde os dispositivos têm poucos recursos, como sensores e dispositivos móveis conectados por redes IoT ou 5G. Em um sistema como o aprendizado federado, com muitos dispositivos colaborando no treinamento de um modelo de IA, a adaptabilidade permite que cada um contribua de maneira eficiente, mesmo em condições variáveis de conexão ou energia.

A adaptabilidade ajuda a IA a funcionar de maneira mais prática e eficiente. Por exemplo, se a conexão de um dispositivo é instável, algoritmos adaptativos podem reduzir a frequência de comunicação com o servidor, como acontece no método **Adaptive Federated Averaging**. Se o dispositivo tem pouca bateria, a compressão dos dados pode ser mais agressiva para economizar energia, mas ainda assim manter uma precisão aceitável, como no caso do **EF-SGD (Error Feedback Stochastic Gradient Descent)**, que compensa a perda de precisão ajustando o modelo nas próximas rodadas.

Outro exemplo de adaptabilidade é o ajuste da taxa de aprendizado, como nos algoritmos **Adam** e **RMSprop**, que ajustam automaticamente a velocidade de aprendizado conforme as mudanças no conjunto de dados e no próprio modelo. Esses ajustes são fundamentais para que o modelo de IA continue aprendendo de maneira estável e eficiente, mesmo com mudanças no ambiente ou nos dados.

A seleção de gradientes mais importantes é outra técnica adaptativa: algoritmos como **Top-k Sparsification** transmitem apenas os gradientes mais significativos para o servidor, ignorando os de menor impacto. Isso economiza largura de banda e recursos de comunicação, o que é útil em dispositivos com conectividade ou energia limitadas. Em dispositivos IoT, técnicas de monitoramento de recursos, como **DynSparse**, adaptam o uso de energia e processamento em tempo real, permitindo que o dispositivo ajuste automaticamente seu desempenho e continue participando do aprendizado federado, mesmo quando a bateria está baixa.

Essas técnicas adaptativas tornam a IA mais eficiente e acessível em dispositivos variados e em condições diferentes, economizando recursos, permitindo que mais dispositivos participem do aprendizado, e mantendo a precisão do modelo. A adaptabilidade é fundamental em ambientes de aprendizado federado, pois permite que o sistema responda às condições variáveis de dispositivos IoT e redes 5G, maximizando o desempenho e a economia de recursos em cenários práticos.

APÊNDICE 6

Termo de Aceite de Entrega

Objetivo deste documento

Este documento faz parte do Processo da disciplina Residência em IA e tem como objetivo formalizar o aceite da entrega considerando o planejado e o realizado para o período.

Data da Reunião ("gate") de aprovação: 6 de nov. de 2024

Participantes da Entrega [matriculados em Residência em IA]:

Francieli Moreira de Carvalho

Entrega: [descrever a ENTREGA: requisitos e produtos gerados: links para textos, códigos, vídeos etc.]

Para esse **gate**, me aprofundei um pouco mais sobre variáveis e os fatores que impactam a **Compressão de Gradientes** no contexto do Aprendizado Federado, com um foco particular em dispositivos conectados via redes 5G.

Além disso, continuei estudando as **métricas de avaliação** usadas para analisar a eficácia e a eficiência dos métodos de compressão, percebendo que métricas como o **tempo de convergência** e a **redução de comunicação** são fundamentais para avaliar a eficiência no uso de recursos.

Estudei também um tutorial de Aprendizado Federado utilizando **Flower** e **TensorFlow**, explorando o funcionamento desse tipo de aprendizado, desde a divisão de dados até a configuração de clientes e a avaliação do modelo. No código, uma rede neural convolucional simples foi treinada para classificar o dataset **MNIST** em um ambiente federado, onde o servidor central combina os pesos dos modelos treinados localmente em cada cliente, mantendo a privacidade dos dados.

Material:

- ➔ V07_estudos de FL - Documentos Google
- ➔ Teste_Aprendizado_Federado_FLower_TensorFlow.ipynb - Colab

Planejamento: [descrever o que pretende fazer para realizar a próxima ENTREGA]

Com base no tutorial de Aprendizado Federado que realizei usando o Flower e TensorFlow, começar a aplicar técnicas de Compressão de Gradientes.

Observação: [caso precise fazer alguma observação, de qualquer "natureza"]

ACEITE DA ENTREGA:

CEDRIC LUIZ DE CARVALHO: Go!

[Documentos citados no Termo de Aceite de Entrega de 06 de novembro]

Variáveis que Influenciam a Compressão de Gradientes

Este documento explora as principais variáveis que afetam a Compressão de Gradientes Adaptativa em um sistema de aprendizado federado, especialmente em contextos onde dispositivos móveis e redes 5G são utilizados. A Compressão de Gradientes Adaptativa busca ajustar a quantidade de dados transmitidos entre os dispositivos e o servidor central de forma dinâmica, com base nas condições específicas de cada dispositivo e da rede. Esse processo visa equilibrar a eficiência da comunicação e o consumo de recursos com a precisão do modelo, proporcionando uma experiência otimizada e adaptável para diferentes dispositivos.

Qualidade da Conexão 5G

A qualidade da conexão 5G desempenha um papel crucial na compressão de gradientes em sistemas de aprendizado federado. Essa variável representa a velocidade, latência e estabilidade da conexão de rede que o dispositivo utiliza para se comunicar com o servidor central. Quando a conexão é de baixa qualidade, com alta latência ou interrupções frequentes, pode ser necessário aplicar uma compressão mais intensa nos dados transmitidos. Isso reduz o volume de dados que precisam ser enviados, diminuindo o risco de falhas na transmissão e garantindo que o dispositivo consiga enviar atualizações mesmo em condições adversas. Por outro lado, quando a conexão é estável e rápida, a necessidade de compressão diminui, permitindo uma transmissão de dados mais precisa e com menor perda de informação, o que beneficia a qualidade do modelo final. Medir essa variável envolve monitorar a latência média, a taxa de upload e download, e a frequência de desconexões. Com base nessas medições, a compressão de gradientes pode ser ajustada dinamicamente para se adaptar às condições de rede, otimizando a eficiência do sistema.

Nível de Bateria do Dispositivo

Outro fator essencial que influencia a compressão de gradientes adaptativa é o nível de bateria do dispositivo. Em sistemas de aprendizado federado, o consumo de energia pode ser um desafio, especialmente em dispositivos móveis que dependem de bateria.

Dispositivos com pouca carga podem precisar de uma compressão mais intensa para reduzir o processamento e a quantidade de dados enviados, o que ajuda a economizar energia. Ao reduzir o volume de dados a serem processados e transmitidos, o dispositivo usa menos energia, prolongando o tempo de uso antes de precisar ser recarregado. Em contrapartida, dispositivos com nível de bateria alto podem operar com uma compressão menos agressiva, permitindo uma maior precisão nos dados transmitidos sem comprometer a eficiência energética. O monitoramento do nível de bateria, expresso em porcentagem e acompanhado de uma estimativa de tempo restante, permite adaptar o sistema de compressão com base na carga disponível, balanceando o consumo de energia com a necessidade de precisão.

Capacidade de Memória e Processamento

A capacidade de memória e processamento do dispositivo é uma variável crítica em sistemas de aprendizado federado com compressão de gradientes. Dispositivos com limitações de memória ou capacidade de processamento podem ter dificuldades para lidar com grandes volumes de dados não comprimidos. Nesses casos, uma compressão mais intensa é necessária para reduzir a carga de trabalho do dispositivo, evitando sobrecargas e garantindo que ele possa participar do processo de aprendizado federado sem comprometer seu desempenho. Já dispositivos mais potentes, com maior capacidade de memória e processamento, conseguem lidar com volumes maiores de dados e podem operar com uma compressão menos intensa, preservando assim mais informações nos gradientes transmitidos e melhorando a precisão do modelo. Para monitorar essa variável, é essencial acompanhar o uso de CPU e memória durante as operações de compressão e transmissão. Com essas informações, a intensidade da compressão pode ser ajustada para evitar sobrecargas, otimizando o desempenho do sistema de acordo com a capacidade do dispositivo.

Condições de Uso do Dispositivo, como Mobilidade

As condições de uso do dispositivo, incluindo fatores como a mobilidade, também influenciam a compressão de gradientes adaptativa. Dispositivos que estão em movimento, como aqueles usados em veículos ou transportados por usuários, podem enfrentar desafios adicionais, especialmente em termos de estabilidade de conexão. A mobilidade do dispositivo pode resultar em desconexões frequentes ou em variações de sinal, o que torna a transmissão de dados menos confiável. Em cenários de mobilidade, uma compressão mais intensa pode ser benéfica para reduzir o volume de dados e, assim, aumentar as chances de que a transmissão ocorra de maneira estável e contínua, mesmo em condições de sinal variáveis. Dispositivos que estão parados, por outro lado, tendem a ter uma conexão mais estável, permitindo uma compressão menos agressiva. Utilizando sensores internos ou informações de localização, é possível identificar se o dispositivo está em

movimento e ajustar a compressão de gradientes com base na estabilidade da conexão, adaptando o sistema para diferentes condições de uso.

Métricas de Avaliação para Compressão de Gradientes

1. Precisão do Modelo (Accuracy)

A precisão do modelo é uma métrica fundamental para avaliar qualquer técnica de aprendizado de máquina. No contexto da compressão de gradientes, é importante monitorar se a compressão afeta a precisão do modelo final após as iterações de treinamento federado. A compressão excessiva pode levar a uma perda de informações cruciais, resultando em uma menor precisão do modelo. Medir a precisão em intervalos regulares permite acompanhar se a adaptação da compressão está impactando negativamente o desempenho do modelo.

Como medir: Calcular a precisão (ou outras métricas, como F1-score ou AUC, dependendo do problema) nos conjuntos de dados de teste após cada rodada de aprendizado federado.

Taxa de Convergência (Convergence Rate)

A taxa de convergência é uma métrica que mede a rapidez com que o modelo federado atinge uma precisão aceitável ou uma estabilidade de desempenho. Em um ambiente com compressão de gradientes, a taxa de convergência pode ser afetada, pois a perda de informação devido à compressão pode dificultar a atualização precisa dos parâmetros. Uma compressão eficiente deve equilibrar a redução de dados com uma taxa de convergência aceitável.

Como medir: Observar o número de rodadas de treinamento necessárias para que o modelo atinja um determinado nível de precisão ou uma margem de erro mínima.

Eficiência de Comunicação (Communication Efficiency)

A eficiência de comunicação é uma métrica essencial em cenários de aprendizado federado, pois o envio de gradientes pode consumir uma quantidade significativa de largura de banda. A compressão de gradientes visa reduzir o número de bits transmitidos, melhorando a eficiência de comunicação. Essa métrica mede a quantidade de dados

realmente enviados após a compressão, em comparação com a quantidade de dados que seriam enviados sem compressão.

Como medir: Comparar o volume de dados (em bits) transmitidos com e sem compressão ao longo das rodadas de aprendizado. Uma métrica associada pode ser a **taxa de compressão**, que mostra o quanto o volume de dados foi reduzido.

Consumo de Energia (Energy Consumption)

O **consumo de energia** é uma métrica especialmente importante para dispositivos móveis, que frequentemente participam do aprendizado federado e têm restrições de bateria. A compressão de gradientes adaptativa pode ajudar a economizar energia, reduzindo o volume de dados e o processamento necessário para transmitir e receber gradientes. Medir o consumo de energia durante o processo de compressão permite avaliar se a técnica está realmente beneficiando o dispositivo.

Como medir: Monitorar o consumo de energia do dispositivo durante o treinamento e a comunicação dos gradientes. Ferramentas específicas de medição de energia podem ser usadas para obter dados precisos sobre o impacto da compressão no consumo de bateria.

Taxa de Perda de Informação (Information Loss Rate)

A taxa de perda de informação mede o quanto de precisão ou relevância dos gradientes originais foi perdida após a compressão. Esse tipo de métrica é essencial para avaliar o impacto da compressão nos dados transmitidos. Embora uma alta compressão reduza o volume de dados, ela também pode remover informações cruciais para o ajuste do modelo, prejudicando a convergência e a precisão.

Como medir: Comparar o valor dos gradientes antes e depois da compressão, observando a diferença média ou a variação absoluta para quantificar a perda de informações.

Robustez em Diferentes Condições de Rede (Network Condition Robustness)

A robustez em diferentes condições de rede avalia como a compressão de gradientes se adapta a variações na qualidade da rede, especialmente em redes móveis, onde a conexão pode ser instável. A compressão de gradientes adaptativa deve ser capaz de ajustar sua intensidade com base na qualidade da conexão (por exemplo, aumento da compressão em redes lentas para minimizar o impacto da perda de pacotes).

Como medir: Testar o desempenho da compressão em várias condições de rede (alta latência, baixa largura de banda, desconexões frequentes) e observar o impacto na precisão do modelo e na eficiência da comunicação.

Latência de Treinamento (Training Latency)

A latência de treinamento mede o tempo necessário para que o dispositivo processe e transmita os gradientes após a compressão. Esta métrica é importante para avaliar o impacto da compressão adaptativa no tempo total de treinamento. Uma compressão mais intensa pode reduzir o volume de dados, mas também pode aumentar o tempo de processamento, criando um trade-off entre latência e eficiência de comunicação.

Como medir: Medir o tempo total necessário para processar, comprimir e transmitir os gradientes em cada dispositivo após uma atualização de parâmetros.

Referências:

[1610.02527] Otimização federada: aprendizado de máquina distribuído para inteligência no dispositivo

[1812.01097] LEAF: A Benchmark for Federated Settings

[1602.05629] Communication-Efficient Learning of Deep Networks from Decentralized Data

APÊNDICE 7

Termo de Aceite de Entrega

Objetivo deste documento

Este documento faz parte do Processo da disciplina Residência em IA e tem como objetivo formalizar o aceite da entrega considerando o planejado e o realizado para o período.

Data da Reunião ("gate") de aprovação: **27 de nov. de 2024**

Participantes da Entrega **[matriculados em Residência em IA]**:

Francieli Moreira de Carvalho

Entrega: **[descrever a ENTREGA: requisitos e produtos gerados: links para textos, códigos, vídeos etc.]**

Para este Gate, foram realizados os seguintes testes:

1. **Aprendizado Federado sem Compressão**
2. **Aprendizado Federado com Compressão de Gradientes Básica**
3. **Aprendizado Federado com Compressão de Gradientes Adaptativa**

Configurações do Experimento:

- **Dataset**: MNIST
- **Modelo Base**: Rede Neural Simples
- **Estratégia Base**: FedAvg
- **Número de Rodadas**: 5
- **Divisão dos Dados**: Uniforme entre 10 clientes

Relatório: Relatório de testes FL - Documentos Google

S/ Compressão: O aprendizado foi consistente entre os clientes, mas o tráfego de gradientes foi elevado.

Compressão de Gradientes: A compressão reduziu o tempo de comunicação entre os clientes e o servidor.

Compressão de Gradientes Adaptativa: A compressão adaptativa preservou melhor as informações importantes nos gradientes, apesar de um leve aumento no tempo de execução em relação à compressão fixa.

Os resultados obtidos estavam dentro do esperado, considerando o objetivo de melhorar a eficiência de comunicação com mínima perda de precisão; no entanto, ressalta-se que o dataset utilizado não pode ser considerado altamente heterogêneo, o que limita a representação de

cenários reais com distribuições de dados não-IID.

Planejamento: **[descrever o que pretende fazer para realizar a próxima ENTREGA]**

- **Utilizar dados não-IID (Non-Independent and Identically Distributed)**
- **Ampliar o número de clientes simulados**
- **Testar diferentes modelos de aprendizado federado além do FedAvg**

Observação: [caso precise fazer alguma observação, de qualquer "natureza"]

ACEITE DA ENTREGA:

LEONARDO ANTÔNIO ALVES: Em análise!

[Documentos citados no Termo de Aceite de Entrega de 06 de novembro]

Objetivo

Este relatório apresenta os resultados preliminares obtidos em testes simulados de aprendizado federado com foco na aplicação de compressão de gradientes adaptativos. O principal objetivo foi avaliar a eficiência da comunicação e sua influência na precisão do modelo em um cenário com dados limitadamente heterogêneos.

Metodologia

Configurei o ambiente de testes em uma máquina com processador Intel Core i5 de quarta geração, 16 GB de memória RAM e sistema operacional Windows 10 de 64 bits. Utilizei o Visual Studio Code como ambiente de desenvolvimento, juntamente com as bibliotecas Python 3.8, TensorFlow 2.x e Flower para a implementação do aprendizado federado.

O dataset escolhido foi o MNIST, composto por 60.000 imagens de treinamento e 10.000 imagens de teste de dígitos manuscritos de 0 a 9. As imagens foram normalizadas para valores entre 0 e 1 e achatadas em vetores de 784 elementos. Dividi os dados de forma independente e identicamente distribuída (IID) entre 10 clientes simulados, com cada

cliente recebendo um subconjunto igual de 6.000 imagens de treinamento e 1.000 imagens de teste. Optei por utilizar dispositivos homogêneos devido à natureza do dataset e ao escopo dos experimentos.

O modelo de rede neural implementado consistiu em uma camada oculta com 64 neurônios e função de ativação ReLU, seguida por uma camada de saída com 10 neurônios e função de ativação Softmax, correspondendo às classes do MNIST. Utilize o otimizador Adam com taxa de aprendizado inicial de 0,001, a função de perda Sparse Categorical Crossentropy e acurácia como métrica de avaliação. O treinamento local em cada cliente foi realizado com tamanho de batch de 32 e apenas 1 época por rodada, considerando o número limitado de rodadas no experimento.

No lado do servidor, apliquei a estratégia de agregação FedAvg (Federated Averaging) sem modificação inicial. Todos os 10 clientes participaram de cada uma das 5 rodadas de treinamento, enviando seus modelos locais para o servidor central após cada rodada.

Descrição dos Testes

Teste 1: Aprendizado Federado Sem Compressão

No primeiro teste, não apliquei nenhuma compressão, servindo como referência para comparação. Os clientes treinavam o modelo localmente e enviavam os parâmetros completos (pesos e vieses) ao servidor, representados em ponto flutuante de 32 bits (float32), resultando em um volume maior de dados transmitidos.

Teste 2: Aprendizado Federado com Compressão Básica de Gradientes

No segundo teste, implementei uma compressão básica de gradientes utilizando quantização uniforme. Antes de enviar os gradientes ao servidor, reduzi a precisão dos valores convertendo-os de float32 para float16 (16 bits) ou int8 (8 bits). Durante o treinamento local, os gradientes eram calculados normalmente. Antes da transmissão, convertia-os para a precisão reduzida, diminuindo assim o volume de dados. No servidor, os gradientes eram reconvertidos para float32 antes da agregação, mantendo a consistência no processo de atualização dos parâmetros. Essa abordagem reduziu o tamanho dos gradientes pela metade ou em 75%, dependendo da precisão utilizada, mas introduziu perdas de informação devido à redução de precisão.

Teste 3: Aprendizado Federado com Compressão Adaptativa de Gradientes

No terceiro teste, implementei uma compressão adaptativa de gradientes, ajustando dinamicamente a taxa de compressão com base nas características dos gradientes. Inicialmente, apliquei um thresholding, onde gradientes com valores absolutos abaixo de um limiar predefinido eram considerados insignificantes e descartados ou representados com menos bits. Calculei o limiar adaptativo com base na magnitude média dos gradientes em cada rodada. Além disso, realizei uma alocação dinâmica de bits, classificando os gradientes por magnitude e atribuindo maior precisão (float32) aos mais significativos, média precisão (float16) aos intermediários e menor precisão (int8) ou descarte aos menos significativos.

Para manter o equilíbrio entre eficiência de comunicação e desempenho do modelo, implementei um feedback loop. Após cada rodada, avaliei as métricas de acurácia e perda. Se verificasse uma redução na acurácia além de um limite aceitável, ajustava os parâmetros de compressão, como o limiar e a alocação de bits, para preservar mais informações nos gradientes nas rodadas subsequentes. Esse processo permitiu adaptar à compressão às necessidades do modelo em tempo real, minimizando o impacto negativo na acurácia enquanto reduzia o volume de dados transmitidos.

Enfrentei desafios ao determinar o limiar adequado e a alocação de bits que não comprometessem significativamente a acurácia. Além disso, a compressão adaptativa introduziu uma sobrecarga computacional adicional nos clientes, o que pode impactar o tempo de treinamento mesmo em dispositivos homogêneos.

Resultados

Após a realização dos três testes, obtive os seguintes resultados em termos de **acurácia média** e **eficiência de comunicação**:

Teste	Acurácia	Volume de dados transmitidos

Sem Compressão	75	32MB
Com Compressão	72	16MB
Compressão Adaptativa	74	12MB

Devido ao número reduzido de rodadas e à simplicidade do modelo, os resultados servem como uma análise preliminar. Em cenários reais, mais rodadas e modelos mais complexos seriam necessários para avaliar plenamente o impacto das técnicas de compressão.

APÊNDICE 8

Termo de Aceite de Entrega

Objetivo deste documento

Este documento faz parte do Processo da disciplina Residência em IA e tem como objetivo formalizar o aceite da entrega considerando o planejado e o realizado para o período.

Data da Reunião ("gate") de aprovação: 5 de dez. de 2024

Participantes da Entrega [matriculados em Residência em IA]:

Francieli Moreira de Carvalho

Entrega: [descrever a ENTREGA: requisitos e produtos gerados: links para textos, códigos, vídeos etc.]

Para este Gate, foram realizados Compressão de Gradientes Adaptativa com dados heterogêneos

Datasets Utilizados:

- **MNIST**
- **CIFAR-10**

Distribuição dos Dados:

- Dados distribuídos de maneira **não-IID (heterogênea)** entre os 10 clientes simulados.

Técnica de Agregação:

- Utilizada a estratégia **FedAvg** para agregação dos gradientes dos modelos locais.

Rede Neural Utilizada:

- **Rede Neural Convolucional Simples (CNN)** com camadas convolucionais e densas.

Testes: Compressão de Gradiente Adaptativo.ipynb - Colab

Planejamento: [descrever o que pretende fazer para realizar a próxima ENTREGA]

Observação: [caso precise fazer alguma observação, de qualquer "natureza"]

Ainda quero melhorar o cenário de dados heterogêneos e testar um modelo de agregação mais robusto, pois tive dificuldades de implementação quando sai de dados homogêneos para heterogêneos.

ACEITE DA ENTREGA:

CEDRIC LUIZ DE CARVALHO: Go!

[Colab com simulações citadas no Termo de Aceite de Entrega de 05 de dezembro]

Link do colab com os experimentos realizados: Compressão de Gradiente Adaptativo.ipynb