Universidade de Pernambuco
Programa de Pós-Graduação em Engenharia da Computação (PPGEC)

Proposta de Tese de Doutorado

Área: Inteligência Computacional

Título Aprendizado Federado Aninhado para Adaptação Contínua de Anomalias

Orientador – Bruno José Torres Fernandes (bjtf@ecomp.poli.br)
Coorientador – Alexander Fabisch (alexander.fabisch@dfki.de)

Descrição – O avanço da tecnologia e a coleta massiva de dados têm impulsionado o desenvolvimento de algoritmos de aprendizado de máquina cada vez mais complexos e eficientes [1]. Entretanto, esses dados frequentemente se encontram distribuídos em múltiplas fontes e domínios, o que dificulta a tarefa de treinar modelos globais capazes de capturar padrões consistentes entre diferentes contextos [2]. Além disso, a centralização de dados, algo recorrente, por exemplo, nos modelos fundamentais (*Foundation Models*) atuais, pode gerar riscos significativos à privacidade e à segurança das informações [3].

O aprendizado federado (Federated Learning – FL) surgiu como um paradigma inovador que permite o treinamento colaborativo de modelos de aprendizado de máquina em conjuntos de dados distribuídos e descentralizados, sem a necessidade de compartilhamento direto dos dados entre os participantes [4]. Essa abordagem viabiliza que múltiplas entidades — como sensores, dispositivos IoT, empresas ou instituições — cooperem na construção de modelos globais, preservando a privacidade e reduzindo os custos de comunicação e armazenamento [5]. O aprendizado federado, portanto, representa uma alternativa promissora para cenários distribuídos, como cidades inteligentes, redes industriais e sistemas de monitoramento de infraestrutura [6][7].

Entre suas principais vantagens, destacam-se a preservação da privacidade [6], a eficiência computacional [7] e o caráter colaborativo [8]. Ao manter os dados nos dispositivos locais, o aprendizado federado reduz riscos de exposição e possibilita o uso de recursos periféricos para treinamento, aliviando a carga dos servidores centrais. Além disso, o modelo federado favorece a cooperação entre múltiplas partes interessadas, mesmo quando seus dados apresentam naturezas ou formatos heterogêneos.

Apesar desses benefícios, o aprendizado federado ainda enfrenta desafios expressivos. A comunicação entre os dispositivos pode se tornar um gargalo em redes com muitos participantes ou conexões instáveis [7]. Também é comum a presença de desequilíbrio de contribuição entre os nós, o que pode comprometer o desempenho coletivo [9]. Outros desafios incluem a tolerância a falhas, a heterogeneidade dos dados e a dificuldade em manter o aprendizado adaptativo diante de mudanças de contexto.

Um caso particularmente desafiador ocorre na detecção de anomalias distribuídas. Em ambientes dinâmicos, como linhas de produção, redes de sensores ou sistemas de segurança, o conceito de “anomalia” pode variar com o tempo e entre diferentes nós. Um evento considerado normal em determinado momento ou local pode tornar-se anômalo em outro. Além disso, em muitos casos, anomalias são identificadas apenas tardiamente por analistas humanos, quando seus efeitos já ocorreram. Essa natureza temporal e contextual das anomalias demanda mecanismos de aprendizado contínuo, capazes de ajustar o modelo global a novas evidências e de incorporar correções retroativas.

Nesse contexto, este projeto propõe desenvolver uma abordagem de Aprendizado Federado Aninhado (Nested Federated Learning) para detecção e adaptação contínua de anomalias. Inspirada na teoria de Nested Learning [11], essa abordagem introduz

múltiplos níveis de aprendizado dentro de cada nó federado, incluindo otimizadores profundos, memórias em diferentes escalas temporais e mecanismos de auto-modificação das regras de aprendizado. Assim, cada modelo local é capaz de aprender, consolidar e adaptar-se a novos padrões anômalos de forma hierárquica e contínua.

Além disso, o projeto busca explorar o conceito de retrocontexto federado, em que anomalias detectadas tardiamente em um nó são incorporadas de volta ao sistema, permitindo a reinterpretação e o ajuste dos modelos locais e globais. Dessa forma, espera-se construir uma arquitetura federada resiliente, capaz de evoluir com o tempo e de responder a mudanças graduais ou repentinas no comportamento dos dados.

Em suma, a proposta visa estender os fundamentos do aprendizado federado tradicional ao domínio do aprendizado contínuo distribuído, combinando eficiência, privacidade e adaptabilidade. Espera-se que os resultados obtidos possam ser aplicados em uma ampla gama de domínios — incluindo manufatura inteligente, monitoramento urbano, saúde digital e sistemas de segurança cibernética — promovendo soluções mais robustas, seguras e evolutivas para os desafios do mundo digitalizado.

Referências Bibliográficas

1. NGUYEN, G. T. et al. Machine learning and deep learning frameworks and libraries for large-scale data mining: a survey. Artificial Intelligence Review, v. 52, p. 77–124, 2019.
2. TULADHAR, A. et al. Building machine learning models without sharing patient data: A simulation-based analysis of distributed learning by ensembling. Journal of biomedical informatics, p. 103424, 2020.
3. ZHANG, T.; HE, Z.; LEE, R. B. Privacy-preserving machine learning through data obfuscation. ArXiv, abs/1807.01860, 2018.
4. MCMAHAN, H. B. et al. Communication-efficient learning of deep networks from decentralized data. In: International Conference on Artificial Intelligence and Statistics. [S.l.: s.n.], 2016.
5. ALEDHARI, M. et al. Federated learning: A survey on enabling technologies, protocols, and applications. IEEE Access, v. 8, p. 140699–140725, 2020.
6. GOSSELIN, R. et al. Privacy and security in federated learning: A survey. Applied Sciences, 2022.
7. SHAHID, O. et al. Communication efficiency in federated learning: Achievements and challenges. ArXiv, abs/2107.10996, 2021.
8. ABHISHEKV, A. et al. Federated learning: Collaborative machine learning without centralized training data. international journal of engineering technology and management sciences, 2022.
9. CUI, S. et al. Collaboration equilibrium in federated learning. Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, 2021.
10. RAMOS, D. B. et al. On the use of scrum for the management of research-oriented projects. Nuevas Ideas en Informática Educativa, n. 12, p. 589–594, 2016.
11. BEHROUZ, A. et al. Nested Learning: The Illusion of Deep Learning Architectures. NeurIPS, 2025.