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

Proposta de Tese de Doutorado

Área: Inteligência Computacional

Título: Transferência de Conhecimento em Aprendizado Federado para Detecção de Gestos Anômalos

Orientador – Bruno José Torres Fernandes (bjtf@ecomp.poli.br)

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]. No entanto, muitas vezes esses dados são distribuídos em diferentes locais, o que torna difícil a tarefa de treinar um modelo com essas informações [2]. Além disso, o compartilhamento desses dados pode violar a privacidade das pessoas ou empresas envolvidas [3].

O aprendizado federado é um paradigma recente [4] que permite o treinamento de modelos de aprendizado de máquina em conjuntos de dados distribuídos e descentralizados, sem a necessidade de compartilhar os dados diretamente entre os participantes. O aprendizado federado permite então que múltiplas entidades (por exemplo, dispositivos móveis, sensores, servidores em diferentes locais) colaborem para treinar um modelo sem compartilhar seus dados brutos. Esta abordagem promove a colaboração entre diferentes entidades, ao mesmo tempo em que protege a privacidade dos dados e minimiza os custos associados à comunicação e ao armazenamento centralizado e pode ser utilizada em diversos cenários, desde segurança urbana até cidades inteligentes [5].

Por outro lado, a detecção de gestos anômalos desempenha um papel importante em áreas como saúde, segurança e interação humano-máquina, permitindo identificar movimentos ou padrões de comportamento que se desviam dos padrões normais. No entanto, a construção de modelos robustos para essa tarefa enfrenta desafios como a escassez de dados rotulados de gestos anômalos e a necessidade de proteger a privacidade dos dados de diferentes fontes [6, 7]. O aprendizado federado é uma solução promissora para lidar com esses problemas de descentralização e a privacidade, permitindo o treinamento colaborativo de modelos sem compartilhamento de dados brutos.

Este projeto propõe o desenvolvimento de uma abordagem que combina aprendizado federado com transferência de aprendizado para detecção de gestos anômalos. A proposta visa adaptar modelos treinados em dados de gestos normais em um domínio para outros contextos, garantindo robustez e eficiência enquanto respeita as restrições de privacidade.

O projeto contribuirá para o avanço na detecção de gestos anômalos em cenários distribuídos, com aplicações práticas em saúde e segurança. Além disso, abordará questões críticas relacionadas à privacidade, eficiência e generalização de modelos em aprendizado federado, alinhando-se aos Objetivos de Desenvolvimento Sustentável (ODS) 3 e 9.

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. Mohammed Aledhari et al., "Federated Learning: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Access*, 2020.
7. Hamza Riaz et al., "Anomalous human action detection using a cascade of deep learning models," *EUVIP Workshop*, 2021.