Universidade Federal de Minas Gerais
Instituto de Ciências Exatas
Departamento de Ciência da Computação

PROGRAMA DE DISCIPLINA

ANO: 2025/1

DISCIPLINA: Proteção da Privacidade em Aprendizado de Máquina
PROFESSOR: Frederico Gadelha Guimarães / Heitor Soares Ramos Filho

CÓDIGO: DCC
CLASSIFICAÇÃO: Pós-graduação/Optativa
CRÉDITOS: 04
CARGA HORÁRIA: TEÓRICA: 60 horas
PRÁTICA: 00 horas
TOTAL: 60 horas
PRÉ-REQUISITO: Conhecimento sólido em aprendizado de máquina, estatística e álgebra linear.

EMENTA: Introdução à privacidade em aprendizado de máquina. Ataques a sistemas de aprendizado de máquina e violações da privacidade. Técnicas de preservação da privacidade. Anonimização e Pseudoanonimização. Aprendizado federado. Privacidade diferencial. Tópicos avançados em privacidade em aprendizado de máquina.

A - OBJETIVOS

Apresentar os desafios e as principais técnicas para preservação e proteção da privacidade em sistemas de aprendizado de máquina, abordando tanto os aspectos teóricos quanto práticos, com foco em algoritmos, frameworks e aplicações. Esta disciplina visa fornecer aos alunos uma base sólida em proteção da privacidade em aprendizado de máquina, capacitando-os a desenvolver sistemas de inteligência artificial que utilizem dados de forma responsável e ética, ao mesmo tempo em que protegem a privacidade dos indivíduos.

B - PROGRAMA

Conteúdo Programático (16 semanas)

Módulo 1: Introdução à Privacidade e Segurança em ML (3 semanas)

- Semana 1: Conceitos básicos de privacidade e segurança da informação. Tipos de dados e informações sensíveis. Legislação e regulamentação sobre privacidade (LGPD, GDPR). Dilemas éticos em ML e privacidade.
- Semana 2: Ataques a sistemas de ML e violações de privacidade: Extração de dados de treinamento, Inferência de informações sensíveis.
- Semana 3: Ataques a sistemas de ML e violações de privacidade: Ataques de

adversários, Envenenamento de dados, Defesas contra ataques adversários.

Módulo 2: Anonimização e Pseudoanonimização (3 semanas)

- Semana 4: Métodos de anonimização de dados (k-anonimato, l-diversidade, t-proximidade).
- Semana 5: Técnicas de pseudoanonimização.
- Semana 6: Limitações e desafios da anonimização e pseudoanonimização. Estudo de casos e aplicações.

Módulo 3: Aprendizado de Máquina Federado (4 semanas)

- Semana 7: Conceitos e princípios do aprendizado federado. Arquiteturas e algoritmos de aprendizado federado (FedAvg, FedSGD).
- Semana 8: Aplicações do aprendizado federado em diferentes domínios (saúde, finanças, etc.).
- Semana 9: Desafios do aprendizado federado: heterogeneidade de dados, comunicação, privacidade e segurança.
- Semana 10: Seminários avançados de aprendizado federado.

Módulo 4: Privacidade Diferencial (4 semanas)

- Semana 11: Fundamentos da privacidade diferencial. Mecanismos de ruído (Laplace, Gaussiano).
- Semana 12: Composição e amplificação de privacidade.
- Semana 13: Aplicações da privacidade diferencial em ML. Bibliotecas para privacidade diferencial (OpenDP, Google Differential Privacy, Opacus).
- Semana 14: Discussão de artigos científicos relevantes na área.

Módulo 5: Tópicos Avançados e Conclusões (2 semanas)

- Semana 15: Seminários sobre Aprendizado de Máquina com Preservação da Privacidade (PPML) para diferentes tipos de dados (imagens, texto).
- Semana 16: Apresentação de projetos e trabalhos dos alunos. Considerações finais sobre o futuro da privacidade em ML.

C - AVALIAÇÃO

- Trabalhos práticos (implementação de técnicas de preservação da privacidade): 40 pt
- Projeto final (desenvolvimento de um sistema de ML com foco em privacidade): 40 pt
- Participação em discussões e apresentação de artigos - 20 pt

C - BIBLIOGRAFIA

1. Katharine Jarmul, Practical Data Privacy: Enhancing Privacy and Security in Data, O'Reilly Media, 2023.

2. Kwangjo Kim, Harry Chandra Tanuwidjaja, Privacy-Preserving Deep Learning: A Comprehensive Survey (Springer Briefs on Cyber Security Systems and Networks), 2021.

3. Artigos científicos relevantes da área

4. Documentação de frameworks e ferramentas para privacidade em ML.