UNIVERSIDADE ESTADUAL DE
MARINGÁ CENTRO DE TECNOLOGIA
DEPARTAMENTO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Disciplina: Tópicos Avançados em Sistemas de Computação	Código: DIN4102
Carga Horária: 60	Número de Créditos: 4
Cursos: Mestrado em Ciência da Computação Doutorado em Ciência da Computação	
Professor: Dr. Bruno Bogaz Zarpelão	

1. EMENTA

Disciplina de conteúdo variável para a introdução de novas tecnologias, visando contemplar assuntos que venham a consolidar a linha de pesquisa.

2. OBJETIVOS

O principal objetivo da disciplina é abordar a interação entre os universos da inteligência artificial e da cibersegurança. Mais especificamente, a disciplina vai buscar: (i) introduzir conceitos de criptografia aplicada, ameaças e controles de segurança; (ii) apresentar e implementar modelos básicos baseados em aprendizado de máquina para a defesa de sistemas computacionais; (iii) apresentar e implementar modelos básicos de proteção à privacidade e segurança voltados para sistemas baseados em aprendizado de máquina.

3. PROGRAMA

1. Ameaças e controles de segurança

2. Criptografia aplicada:
2.1 Cifras simétricas
2.2 Criptografia de chave pública
2.3 Autenticação de mensagens e assinaturas digitais

3. Aprendizado de máquina aplicado a cibersegurança
3.1 Coleta de dados
3.2 Desenvolvimento de modelos de aprendizado de máquina
3.3 Avaliação dos modelos

4. Cibersegurança aplicada a aprendizado de máquina
4.1 Ameaças voltadas a aplicações de inteligência artificial

4.2 Aprendizado federado e privacidade diferencial

4. BIBLIOGRAFIA

Anderson, R. Security Engineering : a guide to building dependable distributed systems. S.L.: John Wiley & Sons, 2020.

Stallings, W. Cryptography and Network Security : principles and practice, global edition. S.L.: Pearson Education Limited, 2022.

Dwork, C.; Roth, A. The algorithmic foundations of differential privacy. Boston: Now Publ, 2014.

Valissev, A. et al. Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. Disponível em: <https://doi.org/10.6028/NIST.AI.100-2e2023>. Acesso em: 3 maio. 2024.

Artigos científicos relacionados ao tema.

5. CRITÉRIO DE AVALIAÇÃO

1ª nota periódica: avaliação escrita cobrindo os tópicos de ameaças, controles de segurança e criptografia aplicada (peso 1).

2ª nota periódica: projeto de implementação cobrindo o tópico de aprendizado de máquina aplicado a cibersegurança (peso 1)

3ª nota periódica: projeto de implementação cobrindo o tópico de cibersegurança aplicada a aprendizado de máquina (peso 1)

Nota final: média aritmética das três notas.

Prof. Dr. Bruno Bogaz Zarpelão

APROVAÇÃO DO CONSELHO ACADÊMICO
DO PROGRAMA DE PÓS-GRADUAÇÃO