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

Proposta de Tese de Doutorado

Área: Computação Inteligente

Título: Antivírus baseado em Rede Neural Artificial dotado de justificativas inteligentes audiovisuais.

Orientador – Sidney Marlon Lopes de Lima (sidney.lima@ufpe.br)

Descrição:

Na era digital, a manipulação social se tornou uma arma poderosa, explorando a vulnerabilidade humana para obter dados confidenciais e causar danos. As medidas tradicionais de segurança, como antivírus e *firewalls*, frequentemente falham em conter essa ameaça, pois não consideram o fator humano. A falta de clareza nas decisões dos sistemas de segurança gera desconfiança e desativação das medidas de proteção pelos usuários. Além disso, a complexidade das técnicas de inteligência artificial dificulta sua implementação em tempo real em dispositivos móveis. Como objetivo, propomos um mecanismo de segurança digital que combina aprendizado de baixa complexidade computacional aliada ao fornecimento audiovisual de justificativas inteligentes e convincentes aos usuários. Essa abordagem oferece como benefício explicações claras e personalizadas, capazes de aumentar a confiança dos usuários nas medidas de segurança.

Materiais e Habilidades necessárias

- Familiaridade com técnicas de redes neurais artificiais visando reconhecimento de padrão.
- Conhecimentos sólidos nas linguagens Python em ambiente de Google Colab.
- Conhecimento quanto à criação de extensão (*add-on*) para navegadores em JavaScript.
- Conhecimento em comunicação *webhook* entre extensão de navegador e ambiente Google Colab.
- Conhecimento básico em edição de imagens do tipo gif.

Referências Bibliográficas

Pinheiro, R.P., Lima, S.M.L., Souza, D.M. *et al.* Antivirus applied to JAR malware detection based on runtime behaviors. Scientific Reports - Nature Research 12, 1945 (2022). https://doi.org/10.1038/s41598-022-05921-5

Lima, S.M.L., Silva, S.H.M.T., Pinheiro, R.P. *et al.* Next-generation antivirus endowed with web-server Sandbox applied to audit fileless attack. Soft Computing 27, 1471–1491 (2023). https://doi.org/10.1007/s00500-022-07447-4