

Projeto 8: Classificação de Ataques de Rede com Random Forest e SVM

- Dataset: CICIDS2017
- Modelos: Random Forest e SVM (comparativo)
- Descrição: Implementar e comparar modelos de Random Forest e SVM para classificar diferentes tipos de ataques de rede em dados de tráfego de rede. Este projeto complexo explora a aplicação de algoritmos de classificação em cibersegurança, um domínio com dados tabulares de alta dimensionalidade e classes desbalanceadas.
- Objetivos de Aprendizado:
 - Implementar técnicas de pré-processamento para dados de tráfego de rede
 - Explorar métodos de seleção de características para reduzir a dimensionalidade
 - Comparar diferentes estratégias de kernel em SVM para dados de rede
 - Analisar a importância de diferentes características no Random Forest
 - Implementar técnicas para lidar com classes desbalanceadas em dados de segurança
- Métricas de Avaliação: Acurácia, precisão, recall, F1-score por classe, matriz de confusão, tempo de treinamento e inferência

O CÓDIGO:

1. Implementação técnica (60%): Correta implementação do modelo e suas particularidades
2. Experimentação e análise (30%): Experimentação com hiperparâmetros, análise de resultados
3. Criatividade e melhorias (10%): Propostas de melhorias ou adaptações criativas ao modelo base

ARTIGO

Deverá ser desenvolvido um artigo pequeno e sucinto, com no máximo 10 páginas, contendo:

1. Introdução - Introduzindo o problema e tarefa a ser desenvolvido;
2. Background - Descrição das tecnologias que serão utilizadas;
3. Métodos - Método proposto, com figuras e dividido por etapas;
4. Resultados e Discussões - Apresentação dos resultados, como modelo utilizado, valores das métricas obtidos e discussão dos resultados;
5. Conclusões - Suas conclusões acerca do trabalho.