

Network Intrusion Detection System by Supervised Machine Learning Technique

Dr. H. Girisha¹, C Lakshmi priya², Bhumika Reddy K S³, Ambika C R⁴, B Varshitha⁵

Associate Professor, Department of Computer Science and Engineering¹

Students, Department of Computer Science and Engineering^{2,3,4,5}

Rao Bahadur Y Mahabaleswarappa Engineering College, Bellary, Karnataka, India

Corresponding author: hosalligiri@rymec.in

Abstract: *Phishing attacks are a growing cybersecurity concern, where attackers impersonate legitimate websites to steal sensitive user information such as login credentials and financial data. Traditional methods like blacklisting are ineffective against newly generated phishing sites. This project introduces Fresh-Phish, an open-source and extendable phishing detection system that leverages machine learning to classify websites as legitimate or phishing. By integrating 29 key features, Fresh-Phish improves upon existing methods by maintaining an updated dataset, optimizing feature selection, and reducing dataset biases. The system employs a Flask-based web interface for user interaction and a Telegram bot for real-time phishing alerts..*

Keywords: Network Security, Intrusion Detection System (IDS), Supervised Machine Learning, Feature Selection, Anomaly Detection, NSL-KDD Dataset, Artificial Neural Network (ANN)

