IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, June 2025
Impact Factor: 7.67

A Novel Ensemble Machine Learning Method to Detect Phishing Attacks

Mr. P. B. Vikhe[1], Mayur Agre[2], Dhruv Yelmame[3], Aryan Bansode[4], Tejas Pansare[5]
Assistant Professor, Computer Department [1]
Student, Computer Department[2,3,4,5]
Pravara Rural Engineering College, Loni, Rahata, India

Abstract: *Phishing remains a major cybersecurity challenge, aiming to trick users into disclosing personal or confidential information through deceptive means. Conventional detection methods often struggle to keep up with the fast-changing nature of these threats. This project introduces an innovative ensemble machine learning framework that enhances phishing attack detection by integrating multiple classification models such as Random Forest, Gradient Boosting, and XGBoost. These models are trained on a balanced dataset containing both phishing and legitimate websites. Important features related to URLs, domain behaviour, and structural elements are extracted to improve model performance. Evaluation based on accuracy, precision, recall, and F1-score confirms that the ensemble approach delivers improved detection rates and stronger resilience against evolving phishing techniques, making it a reliable tool for enhancing digital security.*

Keywords: Phishing Detection, Ensemble Learning, Cybersecurity, Machine Learning, URL Analysis, Classification Models, XGBoost

DOI: 10.48175/IJARSCT-27708