A Filter-Based Feature Selection for Robust Phishing Attack Detection using XGBoost

Isaac Dawandakpoye Ohwosoro

Post Graduate Student, Department of Computer Science

Faculty of Science, Delta State University, Abraka, Nigeria

ohwozik@gmail.com

Abstract: *Phishing attacks are a pervasive cyber threat that has grown in sophistication and scale, presenting significant challenges to cybersecurity professionals. To effectively combat phishing, robust detection mechanisms are crucial, and machine learning has emerged as a powerful tool for this purpose. This study addresses the challenge of creating a fast and reliable framework to counter phishing attacks. We introduce a novel approach that integrates filter-based feature selection methods with the XGBoost algorithm. XGBoost is chosen for its high computational efficiency, outperforming other gradient boosting techniques by a factor of ten, while mutual information gain is used for rapid initial feature selection. Our proposed framework achieves outstanding performance, with an accuracy of 97.0%, precision of 96.3%, recall of 96.5%, F1-score of 96.6%, and ROC AUC score of 99.6%. These results demonstrate the framework's capability to effectively detect and mitigate phishing attacks, providing a timely and powerful tool for enhancing cybersecurity defenses.*

Keywords: XGBoost, Machine learning, filter method Phishing attacks and mutual information gain.