ABSTRAK

ADITYA FIRMANSYAH. Perbandingan Kinerja Algoritma *Random Forest* dan *XGBoost* untuk Klasifikasi URL *Phishing* Obfuskasi. Dibimbing oleh BERTA ERWIN SLAM dan FERDI CHAHYADI.

Perkembangan teknologi yang pesat, menjadikan ancaman *Phishing* terus meningkat, ini menyebabkan ancaman keamanan siber yang serius karena pelaku siber sudah memanfaatkan teknik obfuskasi URL untuk mengelabui sistem deteksi yang ada. Salah satu kelemahan mendasar pada penelitian terdahulu yaitu *Machine Learning* yang digunakan untuk klasifikasi *phishing* masih menggunakan dataset standar, belum menganalisis lebih lanjut terkait URL *Phishing* yang mengandung Teknik obfuskasi. Oleh karena itu, penelitian ini bertujuan untuk membandingkan kinerja algoritma *Random Forest* dan *XGBoost* secara spesifik dalam mengklasifikasikan URL *Phishing* berbasis obfuskasi. Model dievaluasi secara bertahap mulai dari penggunaan *Dataset Pairing* sintetis hingga menggunakan Dataset Organik berimbang guna menguji performa murni algoritma. Evaluasi dilakukan dengan mengekstraksi 6 fitur leksikal pada 12.000 dataset yang dikategorikan kedalam dua kelas dataset, yaitu kelas aman(*Legitimate*) dan kelas *Phishing*. Hasil pengujian final membuktikan bahwa kedua algoritma memiliki performa yang sangat tangguh. Algoritma *Random Forest* maupun *XGBoost* sama-sama sukses mencatatkan tingkat Akurasi yang identik yakni sebesar 94,83%, dengan metrik Presisi tembus diangka 98,82%. Temuan ini membuktikan bahwa *Random Forest* dan *XGBoost* sama-sama terbukti sangat layak diimplementasikan sebagai inti mesin pendeteksi ancaman keamanan *Phishing*.

Kata Kunci: Klasifikasi, Obfuskasi, *Phishing*, *Random Forest*, *XGBoost*, *Trivial Learning*.

ABSTRACT

ADITYA FIRMANSYAH. Performance Comparison of Random Forest and XGBoost Algorithms for Obfuscated Phishing URL Classification. Supervised by BERTA ERWIN SLAM and FERDI CHAHYADI.

The rapid development of technology has caused phishing threats to continuously increase, leading to serious cybersecurity concerns as cybercriminals have utilized URL obfuscation techniques to deceive existing detection systems. A fundamental weakness in prior research is that the Machine Learning used for phishing classification still relies on standard datasets, without further analyzing phishing URLs that contain obfuscation techniques. Therefore, this research aims to compare the performance of Random Forest and XGBoost algorithms specifically in classifying obfuscation-based phishing URLs. The models were evaluated progressively, starting from the use of synthetic Dataset Pairing to a balanced Organic Dataset to test the pure performance of the algorithms. The evaluation was conducted by extracting 6 lexical features on a dataset of 12,000 instances categorized into two dataset classes, namely the Legitimate class and the Phishing class. The final testing results proved that both algorithms possess highly robust performance. Both Random Forest and XGBoost successfully recorded an identical Accuracy rate of 94.83%, with Precision metrics reaching 98.82%. These findings prove that both Random Forest and XGBoost are highly viable to be implemented as the core engines for phishing security threat detection.

Keywords: Classification, Obfuscation, Phishing, Random Forest, XGBoost, Trivial Learning.