Abstrak

Malware telah menjadi sorotan utama dalam keamanan sistem komputer karena penyebarannya yang cepat dan dampak negatifnya terhadap kinerja sistem. Mendeteksi malware kini menjadi sangat penting, salah satunya dengan menggunakan klasifikasi Machine Learning yang mempelajari karakteristik aplikasi tanpa perlu menjalankannya. Dalam penelitian ini, penulis menilai efektivitas deteksi malware dalam analisis statis file Windows Portable Executable (PE) dengan menggunakan algoritma Support Vector Machine (SVM) dan Random Forest. Dengan melatih model-model ini menggunakan kumpulan data yang berisi file PE terkait malware dan aplikasi yang aman, penulis bertujuan untuk mengklasifikasikan file PE sebagai malware atau aman. Tujuan utamanya adalah untuk menentukan algoritma pembelajaran mesin yang paling efektif untuk mendeteksi malware dalam file PE, serta membandingkan kinerja algoritma SVM dan Random Forest. Hasilnya menunjukkan bahwa algoritma Random Forest mencapai tingkat akurasi yang mengesankan sebesar 98,53%, sedangkan algoritma SVM mencapai akurasi 97,14%, sedikit di bawahnya.

Kata kunci: Deteksi Malware, Support Vector Machine, Random Forest, Machine Learning, Windows Portable Executable