ABSTRAK

Perkembangan *malware* sebagai ancaman siber terus meningkat dengan tingkat kompleksitas yang semakin tinggi. Program antivirus konvensional berbasis *signature* mengalami keterbatasan dalam mendeteksi *malware* yang menginfeksi atau menyamar sebagai *file-file legitimate* seperti dokumen Ms. Office dan arsip ZIP. Keterbatasan ini menuntut pengembangan metode deteksi alternatif yang lebih adaptif dan efektif. Analisis statis menggunakan entropi *file* menawarkan solusi strategis untuk mendeteksi *malware* tanpa perlu mengeksekusi *file*, sehingga meminimalkan risiko infeksi sistem.

Penelitian ini mengimplementasikan metode deteksi *malware* berbasis analisis *multiple entropy* yang terdiri dari Entropi Shannon, Entropi Rényi dengan parameter $\alpha=2$ dan $\alpha=5$, serta Entropi Markov. Keempat fitur entropi ini dipilih karena kemampuannya menangkap karakteristik kriptografis *malware* yang cenderung memiliki nilai entropi tinggi, berkisar antara 6 hingga 8. Model *machine learning* Random Forest diterapkan untuk mengklasifikasikan *file* sebagai *malware* atau *benign*, kemudian dibandingkan performanya dengan model Support Vector Machine (SVM) yang telah digunakan dalam penelitian sebelumnya.

Dataset yang digunakan dalam penelitian ini bersifat *imbalanced*, mencerminkan kondisi nyata di mana jumlah *benign file* umumnya lebih banyak daripada *malware*. Evaluasi model dilakukan menggunakan metrik F1-*Score* yang lebih *robust* terhadap ketidakseimbangan data. Hasil eksperimen menunjukkan bahwa model Random Forest mencapai F1-*Score* sebesar 94,58%, melampaui performa model SVM yang memperoleh F1-*Score* 90,82%. Peningkatan performa sebesar 3,76% ini mengindikasikan bahwa Random Forest lebih optimal dalam mengekstraksi dan mengombinasikan pola dari fitur *multiple entropy*.

Penelitian ini membuktikan bahwa penerapan model Random Forest pada analisis statis berbasis *multiple entropy* mampu meningkatkan akurasi deteksi *malware* secara signifikan. Metode ini berpotensi diimplementasikan sebagai mekanisme deteksi proaktif dalam sistem keamanan siber, khususnya untuk mengidentifikasi *malware* yang bersembunyi dalam format *file* umum.

Kata Kunci: *malware*, analisis statis, *multiple entropy*, Shannon, Rényi, Markov, Random Forest, Support Vector Machine, deteksi *file*, *imbalanced dataset*