BAB V
KESIMPULAN DAN SARAN

5.1. Kesimpulan

Penelitian ini membuktikan bahwa model *Decision Tree* adalah alat yang efektif dalam analisis dinamis *malware*, khususnya dalam konteks serangan phishing. Dengan pemahaman yang lebih baik tentang karakteristik dinamis *malware*, peneliti dan praktisi keamanan siber dapat mengembangkan strategi yang lebih baik untuk mendeteksi dan mencegah serangan-serangan tersebut di masa depan.

1. Model *Decision Tree* yang dibangun berhasil mengidentifikasi karakteristik dari *malware* yang terlibat dalam serangan phishing. Dengan menggunakan atribut-atribut seperti file_deletion, total_process_spawned, parent_child_pairs, dan file_modified, model dapat memisahkan sampel-sampel *malware* ke dalam kategori yang berbeda berdasarkan perilaku dinamis mereka.
2. Karakteristik malware yang didapat dari menganalisis *malware* berbasis dokumen dapat diterapkan dalam *decision tree*. Data yang dikumpulkan dari analisis dinamis ini digunakan untuk melatih model *Decision Tree*. Atribut-atribut yang diidentifikasi selama proses analisis diterapkan dalam decision tree untuk membantu dalam pengkategorian *malware*, menunjukkan bagaimana karakteristik ini dapat digunakan secara efektif untuk klasifikasi *malware*.
3. Efektivitas model *Decision Tree* dalam menganalisis dan membagi klasifikasi dari *malware* berbentuk dokumen dalam serangan *phishing* terbukti cukup tinggi. Efektivitas ini dapat dilihat dari nilai *KFold Cross-validation* setinggi 80% dengan akurasi 86 % dan nilai AUC sebesar 88 %. Artinya, model ini memiliki kemampuan generalisasi yang cukup tinggi dan mampu membedakan antara dokumen yang mengandung *malware* dan dokumen lainnya dengan tingkat akurasi yang signifikan. Pendekatan ini memungkinkan deteksi *malware* yang lebih efisien dan cepat dibandingkan dengan metode-metode tradisional.

5.2. Saran

Penelitian ini memberikan kontribusi yang signifikan dalam bidang analisis *malware*, khususnya dalam konteks serangan phishing. Penggunaan model *Decision Tree* dalam analisis dinamis terbukti efektif dan efisien dalam mendeteksi dan menganalisis *malware* berbentuk dokumen. Namun, masih ada ruang untuk pengembangan lebih lanjut, seperti menguji model dengan dataset yang lebih besar dan lebih beragam, serta mengintegrasikan metode analisis lainnya untuk meningkatkan akurasi dan efektivitas model.