BAB V
PENUTUP

5.1 Kesimpulan

Deteksi-analisis malware adalah topik yang sedang berkembang dalam keamanan siber. Setiap tahun, banyak organisasi dan negara menjadi korban serangan malware. Serangan siber berbasis malware dapat menimbulkan konsekuensi yang menghancurkan, termasuk kerugian finansial, penyelundupan data sensitif, dan spionase dunia maya. Pemindai malware dan solusi antivirus konvensional tidak dapat memenuhi kebutuhan perlindungan secara efektif. Untuk tujuan ini, pemeriksaan malware yang berharga membantu memprediksi kerusakan sebelum terjadi dan membangun solusi inovatif untuk menangani insiden malware.

Kinerja pendekatan deteksi yang diusulkan dievaluasi dengan mempertimbangkan langkah-langkah evaluasi yang berbeda. Hasil eksperimen menunjukkan bahwa skor kombinasi antara DNN berbasis perilaku dan pendekatan berbasis heuristik, serta CNN berbasis perilaku dan pendekatan heuristik mempunyai performa yang lebih baik dibandingkan penggunaan metode ML dan DL saja. Visi simetri ini merespons integrasi dan persinggungan dua bidang penelitian yang sedang berkembang pesat: kecerdasan buatan dan keamanan siber untuk mendorong dan memperkuat postur keamanan.

Hasil simulasi dan analisis data yang dilakukan, maka dapat diperoleh suatu kesimpulan bahwa Metode Support Vector Machine dapat digunakan untuk klasifikasi kualitas hasil pengelasan SMAW dalam industry, dengan menggunakan data kualitas pengelasan SMAW, diperoleh model klasifikasi yang baik, hasil pengujian model dengan menggunakan kernel fungsi quadratik menunjukkan hasil akurasi sebesar 96,2%, dan pengujian menggunakan data uji menunjukkan hasil akurasi sebesar 98% dengan menggunakan kernel fungsi quadratik.

Deteksi malware yang dilakukan dengan metode anomali dan menggunakan algoritma Isolation Forest dapat melakukan pendeteksian dengan cukup baik. Data yang digunakan dalam melakukan analisis adalah data terbaru dari dataset lalu

lintas malware yaitu MTA-KDD'19 yang merupakan hasil penelitian Ivan Letteri et al berdasarkan data asli milik organisasi Stratosphere IPS. Data MTA-KDD'19 terdiri dari data legitimate dan data malware yang digabungkan menjadi satu data utuh. Data tersebut kemudian dibagi menjadi data latih dan data uji sebagai bahan pemodelan Isolation Forest. Dalam penelitian ini dapat diambil dua kesimpulan yang diuraikan sebagai berikut:

1. Dari hasil uji coba yang dilakukan terhadap data uji didapatkan hasil akurasi sebesar 47,30%; precision sebesar 93,47; recall sebesar 47,05%; dan f1-score sebesar 62,59%.
2. Sumber daya yang digunakan pada proses deteksi rata-rata menggunakan 33mb dan titik tertinggi penggunaan memori pada 64mb. Dan juga durasi dalam proses menjalankan deteksi adalah kurang lebih 5 detik.

5.2 Saran

Beberapa saran yang diusulkan oleh penyusun untuk penelitian lebih lanjut sebagai berikut :

1) *Malware* merupakan topik yang masih sangat terbuka luas untuk penelitian, pada penelitian ini penulis menggunakan metode *SVM* maka penulis menyarankan untuk penelitian kedepannya menggunakan teknik analisis *malware* dengan metode yang tidak di gunakan pada penelitian ini.

2) *Tools* yang di gunakan pada penelitian ini tidak terlalu akurat dalam mendeteksi, sehingga perlunya perbaikan pada penelitian selanjutnya

3) Untuk penelitian kedepan dapat menggunakan *tools* analisa *malware* lainnya agar dapat membantu mengetahui karakteristik dari sebuah *malware* secara spesifik.