BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berikut ini adalah kesimpulan dari penelitian ini untuk menyelesaikan masalah yang ada:

1. Menurut fitur aktivitas sistem seperti penggunaan CPU, memori, dan *switching* konteks, algoritma *Support Vector Machine* (SVM) berhasil mengklasifikasikan proses sistem operasi menjadi dua kelas yaitu malware dan non-malware.
2. Dengan *accuracy* 99,57%, *Precision* 99,76%, *recall* 99,38%, dan skor F1 99,57%, model yang dibangun menggunakan SVM dengan kernel linear menunjukkan tingkat keakuratan dan konsistensi model dalam mengenali serangan malware.
3. Untuk memastikan bahwa proses pelatihan dan evaluasi model berjalan secara adil dan representatif, distribusi data uji dan latihan yang seimbang (masing-masing 50% untuk setiap kelas) diperlukan.
4. Jumlah kesalahan klasifikasi yang sangat kecil hanya 86 dari 20.000 data uji, terdiri dari 24 hasil positif salah dan 62 false negative salah membuat model ini dianggap sangat akurat untuk mendeteksi aktivitas malware.

5.2 Saran

Berikut ini adalah langkah-langkah yang disarankan oleh peneliti untuk penelitian lanjutan:

1. Agar model lebih tahan terhadap berbagai jenis ancaman, penelitian selanjutnya disarankan untuk menggunakan dataset yang lebih beragam, termasuk berbagai jenis malware atau data real-time dari sistem jaringan.
2. Untuk menentukan model mana yang terbaik untuk deteksi malware, disarankan untuk membandingkan kinerja algoritma SVM dengan algoritma klasifikasi lainnya seperti *Random Forest*, *Decision Tree*, atau *Deep Learning*.
3. Untuk mengukur efektivitasnya secara langsung dalam menangani ancaman keamanan, model SVM yang dikembangkan dapat diuji lebih lanjut dalam sistem deteksi malware nyata atau dalam lingkungan produksi *(real-time monitoring system*).
4. Untuk meningkatkan kinerja model dan mengurangi kesalahan positif dan negatif, parameter SVM seperti kernel, C, dan gamma harus dipelajari lebih lanjut.