# BAB V

# SIMPULAN, IMPLIKASI DAN REKOMENDASI

## 5.1 Simpulan

Berdasarkan penelitian mengenai implementasi optimasi fungsi kernel pada model SVM sebagai model deteksi malware, diperoleh kesimpulan sebagai berikut

1. Berdasarkan hasil evaluasi. dapat disimpulkan bahwa pendekatan deteksi malware menggunakan algoritma SVM memberikan performa yang sangat baik. Model memperoleh *accuracy* sebesar 87%, dengan *precission* sebesar 87%, yang menunjukkan bahwa model tidak mengalami overfitting dan mampu melakukan generalisasi dengan baik terhadap data baru. Selain itu, nilai *recall* sebesar 95% menunjukkan bahwa model sangat efektif dalam mendeteksi aplikasi malware, yang sangat penting dalam konteks keamanan siber agar tidak ada ancaman yang terlewat. Nilai *F1-score* sebesar 91% juga mencerminkan keseimbangan yang sangat baik antara presisi dan recall, yang menegaskan bahwa model tidak hanya akurat tetapi juga konsisten dalam deteksinya (Panman, D. dkk., 2021).
2. Pemilihan fungsi kernel terbukti memiliki dampak signifikan terhadap kinerja model deteksi malware berbasis SVM. Kernel polynomial dan RBF memberikan performa terbaik di seluruh metrik evaluasi (*accuracy*, *precission*, *recall*, dan *F1-score*), masing-masing mencapai nilai hingga 0,91 untuk *F1-score*. Kernel linear masih layak digunakan dengan performa yang stabil, sedangkan kernel sigmoid menunjukkan hasil paling rendah dengan *accuracy* sebesar 56% dengan *precission* dan *recall* masing-masing 67%. Nilai *F1-score* 68% berarti model masih cukup baik dalam mendeteksi malware dan tidak direkomendasikan untuk dataset ini (Panman, D. dkk., 2021). Temuan ini menegaskan pentingnya pemilihan kernel yang tepat dalam membangun sistem deteksi malware yang optimal.

## 5.2 Implikasi

Implementasi optimasi fungsi kernel dalam deteksi malware memiliki dampak yang substansial terhadap peningkatan efektivitas dan efisiensi sistem

keamanan siber. Pemilihan fungsi kernel yang sesuai dapat meningkatkan akurasi deteksi dengan mencocokkan pola data malware dengan pola kernel yang diterapkan, contohnya, penggunaan kernel polinomial untuk menangkap hubungan non-linear yang rumit dalam perilaku malware. Melakukan eksperimen dengan berbagai fungsi kernel seperti RBF, polinomial, dan sigmoid menjadi krusial untuk menemukan kernel yang paling tepat untuk dataset tertentu, mengingat tidak semua fungsi kernel akan memberikan hasil yang optimal untuk setiap jenis malware.

Analisis kesesuaian pola data malware dengan fungsi kernel merupakan aspek krusial untuk mencapai deteksi yang maksimal. Pemahaman yang mendalam mengenai karakteristik data malware serta pola perilaku yang muncul sangat berperan dalam pemilihan fungsi kernel yang mampu meningkatkan efektivitas deteksi. Dalam beberapa situasi, pengembangan fungsi kernel kustom yang dirancang khusus untuk mengatasi pola malware yang spesifik dapat menjadi solusi yang efisien, sehingga model dapat mengidentifikasi ancaman yang sebelumnya tidak terdeteksi oleh kernel konvensional.

Dengan akurasi yang lebih tinggi, efisiensi deteksi malware meningkat secara signifikan. Hal ini mengurangi jumlah false positives dan false negatives, yang pada gilirannya menghemat waktu dan sumber daya yang dibutuhkan untuk investigasi ancaman. Model yang lebih akurat dan efisien memungkinkan tim keamanan untuk merespons ancaman dengan lebih cepat dan tepat. Hasil yang lebih kuat memungkinkan generalisasi deteksi pada berbagai jenis dataset malware, sehingga memberikan perlindungan yang lebih luas dan menyeluruh. Hal ini menunjukkan bahwa model yang dikembangkan tidak hanya efektif untuk satu jenis dataset, tetapi juga dapat diterapkan secara lebih luas pada berbagai tipe malware, yang pada gilirannya meningkatkan ketahanan dan keandalan sistem keamanan. Implikasi ini menekankan pentingnya pendekatan yang cermat dan berbasis data dalam pemilihan serta penggunaan fungsi kernel untuk meningkatkan kinerja dan efisiensi dalam deteksi malware.

## 5.3 Rekomendasi

Berdasarkan hasil penelitian dalam pengujian terdapata beberapa rekomendasi yang diusulkan untuk penelitian selanjutnya, diantaranya sebagai berikut:

1. Penggunaan pendekatan dinamis atau hibrida pada deteksi malware dengan implementasi ML.
2. Menggunakan metode seleksi fitur yang berbeda atau menggabunkan beberapa metode fitur seleksi.
3. Melakukan penelitian lebih lanjut mengenai perancangan fungsi kernel pada deteksi malware dengan pendekatan dinamis atau hibrida.