

BAB V

KESIMPULAN DAN SARAN

5.1 KESIMPULAN

Penelitian ini telah melalui serangkaian tahapan mulai dari pengumpulan dan eksplorasi data, pemrosesan awal, pemodelan, hingga evaluasi terhadap performa model. Berdasarkan seluruh proses tersebut, beberapa poin penting yang dapat disimpulkan adalah sebagai berikut:

1. Model klasifikasi berbasis *random forest* berhasil dibangun untuk mendeteksi serangan *dictionary brute force* pada jaringan IoT menggunakan *dataset* CICIoT2023. Model ini menunjukkan performa yang sangat baik dengan akurasi mencapai 96.45% pada skenario tanpa seleksi fitur.
2. Penerapan seleksi fitur menggunakan metode *recursive feature elimination* menghasilkan model yang lebih ringkas tanpa penurunan performa signifikan. Model dengan 10 fitur terpilih bahkan menunjukkan sedikit peningkatan akurasi menjadi 96.51%, yang menandakan efektivitas seleksi fitur dalam menyederhanakan model.
3. Eksperimen tambahan yang dilakukan melalui variasi konfigurasi seperti rasio data latih dan uji, rasio *balancing data*, jumlah fitur yang dipilih, serta subset fitur dari berbagai pendekatan menunjukkan bahwa hasil model sangat dipengaruhi oleh strategi *preprocessing* dan pemilihan fitur yang tepat. Beberapa kombinasi memberikan hasil lebih optimal, baik dari segi akurasi maupun efisiensi komputasi.

5.2 SARAN

Berdasarkan hasil dan temuan yang diperoleh selama penelitian, beberapa saran yang dapat diberikan untuk penelitian selanjutnya adalah:

1. Disarankan untuk melakukan eksplorasi lebih lanjut terhadap *tuning hyperparameter* baik pada model *random forest* maupun pada proses RFE untuk meningkatkan performa model secara optimal.
2. Penelitian selanjutnya dapat mempertimbangkan untuk menguji model pada lalu lintas *real-time* atau data aktual IoT, guna menilai performa model dalam situasi nyata.
3. Perlu dilakukan perbandingan dengan metode lain seperti SVM, XGBoost, atau *deep learning*, untuk memperoleh perspektif yang lebih komprehensif terhadap keunggulan dan keterbatasan metode *random forest* dan RFE.
4. Sebaiknya dilakukan eksplorasi fitur tambahan atau teknik rekayasa fitur (*feature engineering*) untuk memperkaya informasi yang digunakan oleh model dalam klasifikasi serangan.

