BAB V

PENUTUP

5.1 KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, hasil pengujian dan analisis menunjukkan bahwa algoritma *Naïve Bayes* dapat mendeteksi serangan *Mirai* pada perangkat IoT dengan tingkat akurasi yang sangat tinggi. Model ini mencapai 99,96% untuk data uji tanpa pelatihan model dan 99,95% untuk data latih, menunjukkan efektivitas *Naïve Bayes* dalam klasifikasi serangan pada lingkungan IoT. Hal ini menegaskan bahwa algoritma *Naïve Bayes* memiliki potensi besar dalam meningkatkan keamanan perangkat IoT terhadap serangan *Mirai* yang berbahaya. Dengan tingkat akurasi yang tinggi, metode ini berpotensi menjadi solusi yang efektif dalam mendeteksi dan mengidentifikasi ancaman siber di lingkungan IoT, sehingga dapat meningkatkan keamanan dan ketahanan sistem terhadap serangan seperti *Mirai*. Maka dapat disimpulkan sebagai berikut :

1. *Naïve bayes* merupakan metode yang efektif dalam mendeteksi serangan *Mirai* pada jaringan *Internet of Things* (IoT), berkat pendekatannya yang berbasis probabilitas dan kemampuannya dalam mengklasifikasikan serangan dengan akurasi tinggi.
2. Berdasarkan hasil evaluasi kinerja, algoritma *naïve bayes* menunjukkan performa yang sangat baik dalam mendeteksi serangan *Mirai* pada jaringan IoT, dengan tingkat akurasi yang sangat tinggi. Evaluasi dilakukan menggunakan

classification report dan *k-fold cross-validation*, yang mengonfirmasi efektivitas model dalam mengklasifikasikan serangan.

5.2 SARAN

Meskipun penelitian ini telah menunjukkan hasil yang menjanjikan, masih terdapat beberapa area yang dapat ditingkatkan untuk meningkatkan efektivitas deteksi serangan *Mirai*. Berikut adalah beberapa saran untuk penelitian selanjutnya:

1. Penelitian selanjutnya dapat dilakukan dengan melakukan *cleaning* data yang lebih matang, misalnya melakukan *feature selection* yang relevan pada dataset agar membantu dalam membedakan antara trafik normal dan serangan, serta menghindari *overfitting*.
2. Kedepannya, penggunaan algoritma lain dapat dieksplorasi untuk meningkatkan performa deteksi serangan *Mirai* pada jaringan IoT. Berbagai algoritma *machine learning* lainnya, seperti *Random Forest*, *Support Vector Machine (SVM)*, atau *Deep Learning*, berpotensi memberikan hasil yang lebih optimal dibandingkan *Naïve Bayes*, terutama dalam menangani data yang lebih kompleks dan bervariasi.
3. Jika memiliki fitur kategorikal, pastikan untuk melakukan encoding yang tepat (misalnya, *one-hot encoding*) sebelum menggunakan *Naive Bayes*. Karena *naïve bayes* tidak dapat melakukan deteksi yang lebih besar dari data *float64*.
4. Melakukan *exploratory data analysis (EDA)* untuk memahami struktur, karakteristik, dan pola dalam data sebelum diterapkan pada model *machine*

learning. Dengan melakukan EDA yang baik, hasil prediksi model deteksi serangan *Mirai* dapat lebih akurat dan andal dalam lingkungan IoT.