BAB V

PENUTUP

5.1 KESIMPULAN

Dari hasil penelitian yang telah dilakukan oleh penulis mengenai DETEKSI SERANGAN DDOS PADA *Internet of Things* (IoT) menggunakan *dataset* CiCIoT2023 dari *Canadian Institute for Cybersecurity* (CIC), yang terdiri dari 238.644 baris data dengan 48 atribut. dengan menerapkan algoritma *Naive Bayes*, penulis dapat menyimpulkan sebagai berikut:

1. Dengan dilakukannya penelitian ini dapat menerapkan algoritma *Naive Bayes* untuk mengklasifikasi pola serangan *Distributed Denial of Service* (DDoS) pada lingkungan *Internet of Things* (IoT). Dengan mengunakan 4.615 (80%) *data training*, 1.154 (20%) *data testing* dengan akurasi sebesar 99,83% menunjukkan bahwa model stabil dan konsisten dalam mengenali pola pada data yang diuji.
2. Penerapan algoritma *Naive Bayes* dalam klasifikasi serangan DDoS pada lingkungan IoT berhasil menunjukkan efisiensi dan akurasi yang tinggi, melindungi sistem IoT dari ancaman. Hasil penelitian ini memungkinkan pengembangan lebih lanjut, seperti pengujian pada serangan DDoS yang lebih kompleks, dengan penggunaan *dataset* yang lebih besar dan beragam. Penelitian ini berhasil menerapkan algoritma *Naive Bayes* untuk mendeteksi serangan DDoS pada *Internet of Things* (IoT). Algoritma ini mampu menganalisis pola serangan dengan akurasi yang tinggi sehingga mampu

meningkatkan keamanan sistem pada perangkat dengan sumber daya terbatas.

5.2 SARAN

Penelitian ini telah berhasil mengidentifikasi serangan DDoS pada lingkungan *Internet of Things* (IoT) menggunakan algoritma *Naive Bayes*. Namun, terdapat beberapa keterbatasan yang dapat menjadi peluang pengembangan lebih lanjut. Oleh karena itu, berikut adalah beberapa saran yang diharapkan dapat membantu penelitian selanjutnya untuk mencapai hasil yang lebih baik dan mendalam:

1. Disarankan untuk mengeksplorasi *dataset* yang lebih besar dan mencakup serangan DDoS lainnya. Hal ini akan membantu meningkatkan performa model dalam mendeteksi berbagai jenis serangan DDoS
2. Disarankan untuk mengeksplorasi algoritma lain seperti *Random Forest*, *Support Vector Machine* (SVM), atau *Deep Learning* untuk dibandingkan dengan algoritma *Naive Bayes* dalam hal performa dan akurasi pada deteksi serangan DDoS
3. Disarankan untuk menerapkan metode *cross-validation* agar evaluasi model lebih *robust* dan andal. Dalam memberikan kontribusi penting dalam mendeteksi serangan DDoS pada IoT agar sistem deteksi serangan menjadi lebih akurat, efisien, dan dapat diandalkan untuk menghadapi ancaman di masa depan.