BAB V

SIMPULAN DAN SARAN

5.1 Simpulan

Kesimpulan yang didapatkan dari hasil penelitian ini untuk menjawab permasalahan yang ada adalah :

1. Fitur Terbaik pada dataset adalah *SYN Flag cnt*, dengan nilai korelasi terhadap label sebesar 0.40, adapun fitur yang memberikan pengaruh besar dalam mendeteksi serangan dengan akurasi tertinggi pada tiap algoritma adalah fitur *Flow Pkts/s (Accuracy: 80.89%)* pada algoritma KNN dan fitur *SYN Flag Cnt (Accuracy: 71.94%)* pada algoritma SVM dan NB.
2. Untuk performa tiap algoritma, KNN memiliki performa yang lebih bagus dalam mendeteksi data normal dengan 78.50% presisi dan 87.90% *recall*, dibandingkan mendeteksi serangan dengan 80.21% presisi dan 67% *recall*, persentase akurasi deteksi KNN adalah 79%. SVM memiliki performa yang seimbang antara kelas normal dan serangan dengan presisi 84.87% pada kelas normal dan 83.83% serangan juga *recall* 88.95% pada kelas normal dan 78.32% pada kelas serangan, akurasi pendeteksiannya juga lebih tinggi daripada KNN dengan persentase 84%. NB memiliki performa yang cukup dalam mendeteksi alarm palsu dengan *recall* mencapai 87.85% dan presisi 74.38% namun NB kurang sensitif dalam mendeteksi

serangan sehingga banyak yang terlewatkan dalam mendeteksinya dengan persentase recallnya hanya 58.63%, NB memiliki persentase akurasi sebesar 75%.

3. Untuk kinerja setiap model dalam mendeteksi serangan *botnet* dan data normal, KNN memiliki kinerja yang baik dalam mendeteksi data normal dibandingkan serangan botnet dengan 1289 alarm palsu dan 2565 serangan yang tidak terdeteksi. SVM memiliki kinerja yang seimbang dalam mendeteksi data normal dan serangan dengan 1177 alarm palsu dan 1689 serangan yang tidak terdeteksi. NB memiliki kinerja yang cukup dalam mendeteksi kelas normal tetapi sangat buruk dalam mendeteksi serangan dengan 1294 alarm palsu tetapi 3223 serangan yang tidak terdeteksi.
4. Untuk perbandingan efektifitas antara ketiga algoritma dalam mendeteksi serangan, SVM memberikan performa sekaligus kinerja terbaik dalam mendeteksi serangan dengan *F1-Score* 80% untuk mendeteksi serangan dan akurasi mencapai 84%, selanjutnya diikuti oleh KNN dengan *F1-Score* 73% untuk mendeteksi serangan dan akurasi 79%, NB menempati posisi terakhir dengan *F1-Score* 66% untuk mendeteksi serangan dan akurasi 75%.

5.2 Saran

Peneliti menyarankan untuk penelitian selanjutnya, hal yang bisa dilakukan :

1. Menambahkan metode fitur seleksi baru seperti metode *embedded* atau metode *wrapper* untuk membandingkan hasilnya dengan metode *filter* yang peneliti

gunakan. Menggunakan algoritma lain seperti *random forest* dan *decision tree* untuk membandingkan kinerja dengan model yang ada.

2. Menguji model dengan dataset lainnya seperti *CICIDS* dan *UNSW-NB15* untuk meningkatkan validitas model.
3. Menerapkan algoritma deteksi *botnet* kedalam sistem keamanan jaringan untuk menganalisis data secara *real time.*