BAB V
PENUTUP

5.1 **Kesimpulan**

Penelitian ini dilakukan untuk melakukan penilaian kinerja dari klasifikasi dengan menggunakan fitur wrapper untuk mengetahui proses paling dominan yang bisa dijadikan referensi untuk mendeteksi adanya indikasi dari firewall adaptive itu sendiri.

- Penggunaan *Sequential Forward Selection (SFS)* sebagai fitur wrapper yang digunakan untuk mengetahui fitur paling dominan.
- Algoritma klasifikasi yang digunakan yakni Decision Tree untuk memecahkan permasalahan klasifikasi.
- Berdasarkan eksperimen yang dilakukan menggunakan CICIDS2017 adalah Intrusion Detection Evaluation Dataset dari Kaggle Repository, yang dimana kinerja tertinggi menggunakan sequential forward selection yang menghasilkan kinerja sebesar 99.88%.
- Dari hasil yang didapat jika bernilai 1 adalah dataset normal atau tidak terindikasi serangan sedangkan dataset yang bernilai -1 adalah dataset yang terindikasi serangan atau tidak normal.
- Dari hasil tersebut menunjukan klasifikasi decision tree dengan menggunakan fitur wrapper mampu berkerja secara efisien dan tepat dibandingkan hanya menggunakan klasifikasi tunggal.
- Dari hasil tersebut menunjukan adanya peningkatan akurasi dari penelitian sebelumnya algoritma yang digunakan yaitu decision tree dengan menggunakan fitur wrapper.

Hal ini membuktikan bahwa dengan penanganan yang tepat sebelum proses klasifikasi dapat meningkatkan performa algoritma yang digunakan dalam mengeksekusi dataset.

5.2 Saran

Berdasarkan hasil penelitian ini, ada beberapa saran untuk peneliti yang ingin meneliti lebih lanjut dengan topik yang sama:

1. Mengganti algoritma *Decision Tree* dengan algoritma klasifikasi popular lainnya seperti *Random Forest, Naïve Bayes, Neural Network, K Nearest Neighbor (KNN)* atau *Support Vector Machine*.
2. Menggunakan fitur seleksi lainya, seperti filter dengan menetapkan skor untuk setiap fitur, hybrid feature selection atau fitur seleksi lainnya.
3. Menggunakan proses dimension reduction menggunakan algoritma *Principal Component Analysis (PCA)* sebagai langkah untuk proses ekstraksi fitur
4. Menggunakan metode lain yaitu *Anomal Detection* pada *Supervised Learning* untuk mendeteksi anomali yang terjadi pada dataset *Intrusion Detection Systems (IDSs)* dan *Intrusion Prevention Systems (IPS)*