BAB V

KESIMPULAN

5.1 KESIMPULAN

Berdasarkan hasil eksperimen yang telah dilakukan, kesimpulan yang dapat diperoleh pada penelitian ini diantaranya:

1. Penelitian ini berhasil mengimplementasikan metode *Random Forest* dan *Support Vector Machine* (SVM) untuk mendeteksi serangan *ICMP Flood*. Hal ini dilakukan untuk memanfaatkan kemampuan kedua algoritma dalam mengklasifikasikan data secara efektif, sehingga dapat meningkatkan akurasi dan keandalan sistem dalam mengidentifikasi serta mencegah serangan *ICMP Flood* yang dapat mengganggu keamanan jaringan IoT.
2. Penggunaan *Forward Selection* sebagai pemilihan fitur pada penelitian ini diperoleh 11 fitur terpilih yang akan digunakan pada proses klasifikasi *machine learning* menggunakan metode *Random Forest* dan *Support Vector Machine* (SVM). Hasil eksperimen menggunakan pemilihan fitur *Forward Selection* menunjukkan bahwa ada kenaikan *accuracy* pada saat klasifikasi model *Random Forest* dan SVM. Hasil eksperimen juga memperlihatkan bahwa jumlah fitur sangat mempengaruhi waktu komputasi atau waktu proses, dikarenakan semakin sedikit fitur yang digunakan maka mampu mengurangi beban kerja sistem dalam melakukan proses klasifikasi.

3. Berdasarkan dari hasil implementasi algoritma *Random Forest* dan SVM dalam mendeteksi serangan *ICMP Flood* menunjukkan bahwa metode klasifikasi *Random Forest* merupakan metode dengan performa yang optimal dibandingkan metode klasifikasi SVM. Dari 4 pengujian yang dilakukan, pengujian 2 dengan penggunaan seleksi fitur merupakan pengujian terbaik dari semua pengujian karena model *random forest* mendapatkan *accuracy* sebesar 100% pada setiap mode klasifikasi. Sedangkan untuk model SVM mendapatkan *accuracy* yang lebih baik dengan menggunakan seleksi fitur dengan *accuracy* tertinggi sebesar 99.4508%.

5.2 SARAN

Adapun saran yang dapat penulis sampaikan berdasarkan hasil ekperimen yang telah dilakukan yaitu:

1. Menggunakan metode seleksi fitur yang berbeda untuk mendapat hasil *accuracy* yang lebih baik dengan penggunaan fitur yang relevan.
2. Menggunakan model algoritma yang lain untuk diuji pada *dataset* ini pada penelitian selanjutnya.
3. Menggunakan *split data* yang lebih bervariatif, seperti 60:40 dan 70:30 yang bertujuan mendapatkan komparasi performa yang lebih optimal.
4. Diharapkan bagi penelitian selanjutnya mendeteksi dua atau lebih serangan sehingga mendapatkan hasil yang bervariasi dan lebih baik