BAB 5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan hasil penelitian, implementasi lingkungan simulasi, praproses data, hingga tahap evaluasi terhadap tiga model *machine learning* untuk mendeteksi serangan DDoS pada sistem IoT *Smart Hydroponic* UPNVJ, dapat ditarik beberapa kesimpulan sebagai berikut :

1. Implementasi Machine Learning untuk Deteksi Serangan DDoS.
   Implementasi pendekatan *Supervised Learning* untuk mendeteksi serangan DDoS pada sistem IoT *Smart Hydroponic* FIK UPNVJ dilakukan melalui lima tahapan utama. Proses diawali dengan pengumpulan jaringan mentah berupa perekaman lalu lintas data menggunakan Tshark (5 jam trafik normal dan masing-masing 5 menit untuk 3 skenario serangan DDoS). Selanjutnya, dilakukan pra-filtrasi paket melalui TCP pada port 8000 untuk membuang *background noise* jaringan, diikuti dengan ekstraksi fitur aliran (*flow-based*) menggunakan CICFlowMeter menjadi format `.csv`. Tahap berikutnya adalah pelabelan dan penggabungan data menggunakan Python Pandas untuk mengonversi trafik menjadi 4 kelas target (*multiclassing*) dalam satu master dataset. Alur ini diakhiri dengan pelatihan model menggunakan pembagian rasio data 80:20 pada tiga algoritma, yaitu Random Forest dengan parameter konfigurasi `n_estimators=50, max_depth=5,` dan `random_state=42`, Decision Tree dengan parameter konfigurasi `criterion='gini',max_depth=3,` dan `random_state=42` , dan Support Vector Machine dengan parameter konfigurasi `kernel='linear', random_state=42.`

2. Berdasarkan hasil pengujian, algoritma Support Vector Machine (SVM) dan Random Forest terbukti memiliki efektivitas tertinggi dan paling seimbang dalam skenario klasifikasi multikelas. SVM mencatatkan performa global terbaik dengan nilai *Accuracy* sebesar 98,56%, *Precision* 98,67%, *Recall* 98,48%, dan *F1-Score* 98,57%. Performa ini ditempel ketat oleh Random Forest yang menghasilkan nilai *Accuracy* sebesar 98,29%, *Precision* 98,48%, *Recall* 98,09%, dan *F1-Score* 98,25%. Di sisi lain, algoritma Decision Tree memiliki efektivitas paling rendah di antara ketiganya dengan raihan *Accuracy* 96,50%, *Precision* 96,97%, *Recall* 95,88%, dan *F1-Score* 96,31% karena keterbatasan struktur pohon tunggal dalam memetakan anomali multidimensi yang kompleks pada lapisan aplikasi. Kendati demikian, berdasarkan analisis *Confusion Matrix*, ketiga model tersebut tetap menunjukkan efektivitas sempurna dengan performa klasifikasi mutlak mencapai 100% dalam mendeteksi jenis serangan *TCP SYN Flood*.

5.2. Saran

Untuk pengembangan penelitian lebih lanjut di masa mendatang pada ekosistem keamanan sistem IoT *Smart Hydroponic* FIK UPNVJ, beberapa saran yang dapat dipertimbangkan adalah sebagai berikut:

1. Penambahan Variasi Jenis Serangan
   Penelitian berikutnya dapat memperluas cakupan dataset dengan menambahkan variasi serangan siber lainnya yang relevan dengan ekosistem sistem IoT *Smart Hydroponic* FIK UPNVJ. seperti Botnet IoT dan Injeksi *Firmware* & *Malware*.
2. Implementasi *Continuous Learning* Model *Machine Learning*
   Penelitian selanjutnya disarankan untuk menerapkan pendekatan *continuous learning* atau *lifelong learning* pada model *machine learning* yang digunakan. Pola serangan DDoS dan variasi interaksi data pada arsitektur WebSocket serta REST API dapat berevolusi seiring berjalannya waktu, model tidak boleh bersifat statis.
3. Penerapan Mekanisme Mitigasi Otomatis
   Model machine learning dapat diintegrasikan dengan skrip otomatisasi iptables atau *firewall* server, sehingga ketika model mendeteksi adanya label *HTTP_Flood*, *TCP SYN Flood*, atau *WebSocket Flood*, server dapat melakukan pemblokiran (*drop packet*) secara otomatis terhadap IP penyerang.