BAB 5. PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian mengenai implementasi sistem klasifikasi serangan *Distributed Denial of Service* (DDoS) berbasis *website* dengan komparasi model *Machine Learning*, kesimpulan yang diperoleh sebagai jawaban atas rumusan masalah penelitian adalah sebagai berikut:

1. Hasil komparasi *Logistic Regression*, *Decision Tree*, *Random Forest*, dan XGBoost menggunakan 17 fitur menunjukkan bahwa XGBoost memperoleh performa terbaik dengan *accuracy* 99,9104%, *precision* 99,8187%, *recall* 99,9980%, *F1-score* 99,9083%, ROC-AUC 0,9999, serta skor WSM tertinggi sebesar 0,9547. XGBoost selanjutnya digunakan dalam eksperimen model implementasi. Berdasarkan perbandingan XGBoost 17 fitur dan enam fitur pada pembagian berbasis kelompok enam fitur, model enam fitur memperoleh rata-rata *accuracy* 99,8475%, *recall* 99,9927%, *F1-score* 99,8451%, standar deviasi *accuracy* 0,2727%, dan total 37 *false negative*. Berdasarkan performa, kestabilan, waktu pelatihan, serta jumlah fitur masukan, XGBoost enam fitur ditetapkan sebagai model final untuk integrasi sistem.
2. Sistem klasifikasi serangan DDoS berhasil dirancang, diimplementasikan, dan diuji dalam bentuk aplikasi web lokal berbasis Flask. Sistem mampu menerima dan memvalidasi berkas CSV, memeriksa kelengkapan enam fitur model implementasi, serta menolak data yang mengandung nilai kosong, nonnumerik, NaN, atau *infinite*. Data yang memenuhi ketentuan dapat diklasifikasikan menjadi trafik Normal atau DDoS dan disajikan melalui ringkasan, grafik, probabilitas DDoS, tabel detail, riwayat klasifikasi, serta laporan Excel dan PDF. Detail hasil klasifikasi disimpan dalam berkas CSV, sedangkan metadata riwayat disimpan secara persisten pada basis data SQLite. Hasil *black-box testing* menunjukkan bahwa fungsi klasifikasi, penyajian hasil, pelaporan, penyimpanan riwayat, pembukaan kembali riwayat, dan penghapusan data menghasilkan keluaran sesuai kebutuhan pada lingkungan lokal. Pada pengujian performa lokal, sistem

berhasil memproses berkas hingga 1.000.000 baris dengan rata-rata waktu *backend* sebesar 2,7254 detik dan total waktu pemrosesan serta pembentukan respons *dashboard* sebesar 3,3080 detik. Hasil tersebut berlaku pada satu perangkat dan satu proses klasifikasi dalam satu waktu.

5.2 Saran

Berdasarkan hasil dan keterbatasan penelitian, beberapa saran untuk pengembangan penelitian selanjutnya adalah sebagai berikut:

1. Penelitian berikutnya dapat menggunakan data trafik nyata atau *dataset* dari lingkungan berbeda untuk menguji kemampuan generalisasi model di luar *dataset* simulasi SNT.
2. Sistem dapat dikembangkan untuk klasifikasi multikelas agar mampu membedakan jenis serangan DDoS secara lebih spesifik dengan menggunakan *dataset* yang menyediakan label serangan yang sesuai.
3. Aplikasi dapat diintegrasikan dengan SDN *controller* atau perangkat pemantauan jaringan untuk mendukung klasifikasi secara waktu nyata. Basis data SQLite yang digunakan saat ini juga dapat dikembangkan menjadi basis data berbasis server, seperti PostgreSQL, serta dilengkapi autentikasi, pembagian hak akses, pencatatan aktivitas, dan mekanisme peringatan.
4. Evaluasi lanjutan dapat mempertimbangkan waktu prediksi, penggunaan memori, ukuran model, *false negative*, pengujian keamanan, pengujian beban, dan *usability testing* sebelum sistem diterapkan pada lingkungan produksi.