BAB 5
SIMPULAN DAN SARAN

5.1 Kesimpulan

Penelitian ini bertujuan untuk mengevaluasi dan membandingkan kinerja algoritma Random Forest dan CatBoost dalam mendeteksi serangan DDoS menggunakan dataset CIC-DDoS2019. Proses penelitian melibatkan pengambilan sampel secara seimbang dari lima jenis serangan (LDAP, MSSQL, NetBIOS, Portmap, SYN) serta trafik normal (BENIGN), dilanjutkan dengan preprocessing, encoding label, pembagian data latih dan uji, pelatihan model, evaluasi menggunakan metrik *precision*, *recall*, dan *f1-score*, serta validasi silang untuk mengukur kemampuan generalisasi model.

Berdasarkan hasil eksperimen, diperoleh beberapa poin penting sebagai berikut:

1. **Random Forest** menunjukkan performa yang sangat baik dalam mendeteksi berbagai jenis serangan DDoS dan trafik normal. Model ini mencatat f1-score tertinggi pada label MSSQL (**0,99**), NetBIOS (**0,94**), dan SYN (**0,88**). Selain itu, model ini juga menunjukkan hasil prediksi yang konsisten pada BENIGN (**0,91**).

2. **CatBoost** juga memberikan hasil klasifikasi yang kompetitif, dengan keunggulan pada label BENIGN (**0,96**) dan SYN (**0,94**). Meskipun sedikit tertinggal dari Random Forest pada label LDAP dan Portmap, CatBoost mampu mempertahankan kinerja yang tinggi dan stabil pada hampir seluruh kelas, terutama MSSQL dan NetBIOS yang mencapai f1-score masing-masing **0,99** dan **0,94**.

3. Hasil **visualisasi heatmap** menunjukkan bahwa kedua model memiliki kemampuan klasifikasi multi-kelas yang baik, dengan prediksi yang dominan pada diagonal utama matriks. CatBoost unggul pada kelas normal (BENIGN), sementara Random Forest lebih stabil dalam mengenali serangan LDAP dan Portmap.

4. Evaluasi menggunakan **5-fold cross-validation** menunjukkan bahwa CatBoost mencatat rata-rata f1-score sebesar **0,9270**, precision **0,9334**,

dan recall **0,9292**, yang sedikit lebih tinggi dibandingkan Random Forest dengan f1-score **0,9260**, precision **0,9331**, dan recall **0,9283**. CatBoost juga menunjukkan konsistensi performa antar fold yang lebih baik, menandakan kemampuannya dalam generalisasi terhadap variasi data.

5. Dari sisi efisiensi waktu pelatihan, **Random Forest memiliki keunggulan** dengan waktu pelatihan sebesar **17,29 detik**, dibandingkan CatBoost yang membutuhkan waktu **21,95 detik**. Hal ini menjadikan Random Forest lebih sesuai untuk skenario real-time atau infrastruktur dengan keterbatasan komputasi.

Secara keseluruhan, kedua algoritma mampu mendeteksi serangan DDoS dengan performa tinggi dan konsisten. Pemilihan model dapat disesuaikan dengan kebutuhan sistem, apakah mengutamakan akurasi dan generalisasi (CatBoost), atau efisiensi waktu pelatihan (Random Forest).

5.2 Saran

Berdasarkan hasil dan temuan penelitian, beberapa saran yang dapat diajukan untuk penelitian selanjutnya adalah:

- Penelitian dapat diperluas dengan melibatkan jenis serangan lain dari dataset CIC-DDoS2019, seperti SNMP, UDP, dan UDP-Lag, agar model dapat mengidentifikasi pola serangan yang lebih beragam.
- Penelitian selanjutnya dapat melibatkan model tambahan seperti *XGBoost*, *LightGBM*, atau pendekatan deep learning seperti *LSTM*, untuk mengevaluasi apakah model lain dapat memberikan hasil yang lebih baik atau efisien.
- Evaluasi model dapat diperluas mencakup aspek waktu inferensi dan penggunaan memori, untuk menilai efisiensi model saat diterapkan dalam sistem deteksi serangan secara langsung pada jaringan enterprise.
- Penambahan analisis interpretabilitas model menggunakan metode seperti *SHAP (SHapley Additive exPlanations)* akan berguna untuk memahami kontribusi masing-masing fitur dalam proses klasifikasi.

Dengan penelitian ini, diharapkan dapat memberikan kontribusi nyata terhadap pengembangan sistem deteksi dini serangan DDoS yang lebih akurat, adaptif, dan efisien dalam konteks keamanan jaringan modern.