BAB 5
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil eksperimen dan pembahasan yang telah dilakukan, dapat disimpulkan beberapa hal sebagai berikut:

1. Algoritma XGBoost memiliki kemampuan yang kompetitif dalam mendeteksi aplikasi malware berbasis fitur *permissions*, khususnya dalam konteks klasifikasi biner antara malware dan non-malware. Dengan pemilihan 10 fitur *permissions* terbaik, model mampu melakukan prediksi dengan akurasi tinggi.
2. Masalah ketidakseimbangan kelas (*imbalanced class*) terbukti berpengaruh terhadap penurunan performa model, terutama pada metrik *recall*. Model awal menunjukkan *precision* tinggi (> 0.99) namun *recall* rendah (< 0.42), yang berarti banyak malware tidak terdeteksi. Penerapan parameter *scale_pos_weight*, *threshold tuning*, dan SMOTE mampu meningkatkan sensitivitas model terhadap kelas minoritas (malware), ditunjukkan dengan peningkatan *F1-Score* dan *recall*.
3. Pengujian subset data (500, 1000, 2000) menunjukkan bahwa ukuran data berdampak terhadap stabilitas dan kompleksitas model. Subset kecil seperti 500 menghasilkan hasil yang cepat namun kurang stabil, sementara subset 2000 memberikan performa yang lebih seimbang dan stabil, dengan waktu komputasi yang optimal.
4. Penyesuaian data dan parameter (data-level & parameter-level *tuning*) terbukti lebih berkontribusi dalam menangani ketidakseimbangan kelas dibanding perluasan struktur pohon (*tree*) dalam XGBoost. Hal ini menunjukkan bahwa strategi penanganan imbalance lebih penting dalam konteks klasifikasi malware daripada kompleksitas model itu sendiri.

5.2 Saran

Berdasarkan pelaksanaan dan hasil penelitian ini, beberapa saran yang dapat diberikan untuk pengembangan lebih lanjut adalah sebagai berikut:

1. Perluasan eksperimen dengan kombinasi teknik lain untuk penanganan *imbalance*, seperti *ensemble resampling* atau *cost-sensitive learning*, guna dibandingkan dengan pendekatan *scale_pos_weight*, SMOTE, dan *threshold tuning* yang telah digunakan dalam penelitian ini.
2. Pengujian pada dataset real-world atau terkini, seperti sampel aplikasi dari Google Play Store atau malware terbaru, untuk menguji ketahanan model terhadap data di luar distribusi pelatihan dan meningkatkan *valid*itas eksternal dari model deteksi.
3. Pengembangan untuk klasifikasi multi-kelas dan optimalisasi struktur pohon keputusan, sehingga XGBoost dapat digunakan tidak hanya untuk mendeteksi keberadaan malware, tetapi juga untuk mengklasifikasikan jenis-jenis malware secara lebih spesifik (misalnya trojan, ransomware, spyware). Dalam hal ini, *tuning* jumlah *tree* dan kedalaman maksimal pohon dapat ditelusuri lebih jauh untuk mengakomodasi kompleksitas pola yang berbeda antar jenis malware dengan dataset yang sesuai.