BAB V
PENUTUP

5.1. Kesimpulan

Berdasarkan penelitian yang telah dilakukan, maka dapat diambil kesimpulan:

1. Deteksi *fraud* pada transaksi pembayaran online di PT. XYZ dapat dilakukan dengan memanfaatkan algoritma *Extreme Learning Machine* (ELM). Data yang digunakan mencakup berbagai fitur penting, antara lain *CreatedTime, UpdateTime, Amount, MerchantId, PaymentSource, Status, SettlementAmount, InquiryAmount, DiscountAmount, dan FeeAmount*. Sebelum digunakan dalam pemodelan, data melalui tahapan preprocessing yang meliputi penanganan *missing value*, pelabelan berbasis aturan perusahaan (*rule-based labeling*), *encoding*, pembagian *dataset* dengan rasio 80:20, penanganan outlier, serta standarisasi menggunakan MinMax Scaler. Setelah tahap pelabelan, ditemukan permasalahan ketidakseimbangan kelas, di mana jumlah transaksi *fraud* jauh lebih sedikit dibandingkan transaksi normal. Untuk mengatasi hal tersebut, diterapkan teknik *resampling* dengan metode ADASYN. Dengan demikian, data yang telah diproses dinyatakan siap digunakan untuk pemodelan dengan algoritma ELM.
2. Implementasi *Extreme Learning Machine* (ELM) pada penelitian ini dilakukan dengan dua percobaan dengan memanfaatkan teknik *resampling*, yaitu pemodelan ELM tanpa *resampling* dan ADASYN dengan parameter yang disamakan, yaitu 100 *neuron* pada *hidden layer*, fungsi aktivasi sigmoid, dan bobot awal *seed* 42, agar evaluasi performa setiap percobaan lebih adil. ELM dipilih karena memiliki arsitektur sederhana dengan satu *hidden layer*, sehingga proses pelatihan cepat, efisien untuk data berukuran besar, dan sesuai dengan kebutuhan sistem deteksi *fraud* yang menuntut kecepatan. Untuk meningkatkan transparansi, digunakan LIME yang mampu

menjelaskan kontribusi setiap fitur terhadap hasil prediksi. Contoh dalam penerapan LIME adalah fitur seperti *inquiryAmount* berkontribusi meningkatkan indikasi *fraud*, sedangkan *feeAmount* dan *fraud_rate* justru menurunkannya. Dengan demikian, kombinasi ELM dan LIME menghasilkan sistem deteksi *fraud* yang cepat, akurat, sekaligus mampu memberikan interpretasi yang jelas terhadap faktor-faktor penyebab prediksi.

3. Evaluasi performa sistem deteksi fraud menggunakan algoritma *Extreme Learning Machine* (ELM) menunjukkan bahwa penerapan metode resampling berpengaruh terhadap kinerja model. Pada skenario tanpa *resampling*, nilai *accuracy* mencapai 78.1% dengan *precision* 98.3%, *recall* 78.8%, dan F1-score 87.4%. Setelah dilakukan *oversampling* dengan ADASYN, performa model meningkat, ditunjukkan dengan *accuracy* 82.9%, *precision* 97.8%, *recall* 84.2%, dan F1-score 90.5%. Peningkatan ini menegaskan bahwa ADASYN mampu menyeimbangkan distribusi data sehingga model lebih efektif dalam mengenali transaksi *fraud* tanpa mengorbankan presisi secara signifikan. Berdasarkan hasil tersebut, dapat disimpulkan bahwa algoritma ELM cukup efektif digunakan dalam mendeteksi *fraud*, dan performa terbaik diperoleh melalui penerapan metode *resampling* ADASYN karena mampu meningkatkan *recall* serta F1-score secara konsisten.
4. *Interface* sistem deteksi *fraud* yang dibangun dengan Streamlit berhasil mengintegrasikan algoritma *Extreme Learning Machine* (ELM) dengan *Explainable Artificial Intelligence* (XAI) melalui *Local Interpretable Model-Agnostic Explanations* (LIME). *Dashboard* ini dilengkapi dengan berbagai fitur, mulai dari tahapan *preprocessing data*, analisis data, hingga implementasi XAI LIME. Kehadiran fitur-fitur tersebut memudahkan penyedia layanan untuk memantau transaksi yang mencurigakan sekaligus memahami alasan di balik prediksi model, termasuk identifikasi fitur yang paling berpengaruh terhadap indikasi *fraud*. Dengan demikian, *dashboard*

yang informatif ini tidak hanya berperan sebagai alat deteksi, tetapi juga mendukung proses pengambilan keputusan secara lebih transparan, komprehensif, dan akurat.

5.2. Saran Pengembangan

Penelitian ini memberikan beberapa aspek yang dapat ditingkatkan untuk pengembangan lebih lanjut, antara lain:

1. Memperluas variasi *dataset* dengan menambah periode transaksi dan cakupan merchant yang lebih beragam. Hal ini penting mengingat *dataset* yang digunakan dalam penelitian ini masih berfokus pada aspek-aspek utama, seperti nominal transaksi dan metode pembayaran. Selain itu, penambahan fitur tambahan seperti pola waktu transaksi atau lokasi dapat memberikan informasi yang lebih kaya sehingga model mampu mendeteksi indikasi *fraud* dengan lebih akurat.
2. Pada algoritma Extreme Learning Machine (ELM) pengembangan dapat dilakukan dengan menerapkan proses hyperparameter tuning agar kinerja model lebih optimal. Karena pada penelitian ini hanya berfokus pada parameter default tanpa mencari parameter yang terbaik. Selain itu, penelitian selanjutnya dapat mengombinasikan perbandingan metode *resampling* dengan tuning, serta mencoba pendekatan lain seperti *Deep Learning* dan *Ensemble Learning* untuk meningkatkan performa sistem.
3. Mengintegrasikan metode XAI lain seperti SHAP atau Anchors sebagai pembanding terhadap LIME. Hal ini bertujuan agar hasil interpretasi model lebih beragam dan dapat disesuaikan dengan kebutuhan pengguna, sehingga kejelasan alasan di balik prediksi *fraud* semakin meningkat.
4. *Dashboard* dapat ditingkatkan agar mampu menampilkan analisis transaksi *fraud* secara *real-time*. Dengan adanya fitur ini, sistem tidak hanya berfungsi sebagai media monitoring, tetapi juga sebagai alat deteksi dini yang lebih responsif. Penambahan fitur tambahan seperti filter transaksi, notifikasi otomatis, atau *export* laporan juga dapat meningkatkan kegunaan *dashboard* bagi penyedia layanan.

Halaman ini sengaja dikosongkan