

BAB I PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi digital mendorong peningkatan signifikan pada volume transaksi online setiap tahunnya (Kumala Sari, 2024). Hal ini diperkuat oleh kemunculan berbagai media pembayaran digital yang semakin mempermudah aktivitas ekonomi, salah satunya kartu kredit. Sebagai instrumen pembayaran yang praktis, cepat, dan mendukung ekonomi digital, penggunaan kartu kredit terus mengalami pertumbuhan (Saba Zahid et al., 2024). Namun, peningkatan ini juga diiringi dengan meningkatnya kasus penipuan (*fraud*) pada transaksi kartu kredit (Pantow, 2025). Modus penipuan yang semakin variatif dan kompleks menimbulkan kerugian finansial signifikan bagi perusahaan perbankan maupun nasabah, sekaligus melemahkan kepercayaan masyarakat terhadap sistem keuangan digital (Ofurum, 2024). Oleh karena itu, dibutuhkan sistem deteksi penipuan kartu kredit yang akurat, efisien, dan adaptif terhadap dinamika pola transaksi.

Teknologi *Credit Card Fraud Detection* awalnya banyak mengandalkan metode *machine learning* tradisional yang mampu menganalisis pola transaksi berdasarkan fitur numerik (Ola & Al-Sultan, 2024). Namun, karakteristik transaksi kartu kredit yang sangat dinamis, berdimensi tinggi, serta ketidakseimbangan kelas yang ekstrem, di mana jumlah transaksi fraud jauh lebih sedikit dibandingkan transaksi normal menjadi tantangan utama bagi metode ini (Mizher & Nassif, 2023). Model *machine learning* konvensional sering mengalami penurunan kinerja pada data yang tidak seimbang karena cenderung bias terhadap kelas mayoritas (Yoga Pratama & Ghozi, 2025).

Pendekatan yang lebih mutakhir dan efisien dalam mendeteksi anomali data adalah *deep learning*. Metode ini memiliki kemampuan untuk mengenali pola yang bersifat sekuensial dan kompleks pada dataset, serta mampu mengekstraksi representasi fitur secara mendalam tanpa memerlukan proses seleksi fitur secara manual serta, *deep learning* juga efektif untuk diterapkan pada data berskala besar dan berdimensi tinggi (Y. Chen et al., 2025). Namun demikian, penerapan *deep*

learning dalam sistem deteksi kecurangan kartu kredit masih tergolong terbatas. Hal ini disebabkan oleh kebutuhan sumber daya komputasi yang tinggi, yang dapat menjadi hambatan bagi institusi keuangan dalam implementasinya serta, sifat *black box* dari model *deep learning* menjadikannya sulit diinterpretasikan dan kurang transparan, sehingga menimbulkan tantangan dalam aspek kepercayaan dan akuntabilitas sistem deteksi kecurangan berbasis teknologi ini (Gbeminiyi Deborah Onipede, 2022).

Sebagai upaya untuk mengatasi keterbatasan *deep learning* dalam hal interpretabilitas dan efisiensi komputasi, *ensemble learning* diperkenalkan sebagai strategi untuk meningkatkan performa deteksi dibandingkan mode tunggal dengan menggabungkan keunggulan beberapa model. Dengan menggabungkan model algoritma, sistem deteksi *fraud* dapat menjadi lebih robust, stabil, dan adaptif terhadap variasi pola transaksi yang kompleks.

Berdasarkan tantangan tersebut, penelitian ini bertujuan untuk mengevaluasi performa *ensemble model deep learning* dan *machine learning* dalam mendeteksi penipuan kartu kredit. Model *deep learning* seperti LSTM dan GRU digunakan untuk menangkap pola temporal dan sekuensial pada data transaksi dan model *machine learning*, Random Forest dan AdaBoost digunakan sebagai *baseline model*. Selanjutnya, Multi-Layer Perceptron (MLP) digunakan sebagai *meta-learner* untuk mengintegrasikan prediksi dari berbagai model ke dalam sistem *stacking ensemble*.

1.2. Rumusan Masalah

- 1) Bagaimana kinerja model *deep learning* (seperti LSTM dan GRU) dalam mendeteksi pola sekuensial dan kompleks pada data transaksi kartu kredit yang bersifat tidak seimbang?
- 2) Bagaimana performa model *ensemble machine learning*, seperti Random Forest dan AdaBoost, dibandingkan dengan model *ensemble deep learning* dalam mendeteksi transaksi bersifat *fraud*?

- 3) Se jauh mana pendekatan *stacking ensemble* dengan Multi-Layer Perceptron (MLP) sebagai *meta-learner* dapat meningkatkan hasil deteksi dibandingkan model tunggal?
- 4) Bagaimana perbandingan kinerja model *stacking ensemble deep learning* dan *stacking ensemble machine learning* dalam mendeteksi kecurangan kartu kredit pada data tidak seimbang?

1.3. Batasan Masalah

- 1) Penelitian ini hanya berfokus pada deteksi penipuan transaksi kartu kredit (*credit card fraud detection*) dengan menggunakan pendekatan *ensemble learning*, baik dari model *deep learning* maupun *machine learning*.
- 2) Model *deep learning* yang digunakan dalam penelitian ini dibatasi pada LSTM (Long Short-Term Memory) dan GRU (Gated Recurrent Unit), sedangkan model *machine learning* yang digunakan dibatasi pada Random Forest dan AdaBoost.
- 3) Penelitian ini membatasi penggunaan MLP (Multi-Layer Perceptron) sebagai *meta-learner* dalam metode *stacking ensemble* untuk menggabungkan prediksi dari berbagai model.
- 4) Dataset yang digunakan merupakan dataset transaksi kartu kredit yang memiliki ketidakseimbangan kelas (*imbalanced dataset*), dan penelitian ini tidak mencakup teknik *balancing dataset* di luar konteks model *ensemble*.
- 5) Evaluasi performa model dibatasi pada metrik evaluasi klasifikasi seperti akurasi, *precision*, *recall*, dan *F1-score*, serta tidak mencakup aspek non-teknis seperti faktor keamanan sistem atau pengalaman pengguna.
- 6) Penelitian ini tidak membahas aspek *real-time implementation* dari sistem deteksi fraud, dan hanya berfokus pada pengujian model secara offline menggunakan data historis.

1.4. Tujuan Penelitian

Tujuan dari penelitian ini adalah mencari pendekatan paling efektif dalam mendeteksi transaksi yang tidak sah, serta memahami keunggulan tiap algoritma *deep learning* dan *machine learning*

- 1) Menganalisis kemampuan model deep learning, yaitu LSTM (Long Short-Term Memory) dan GRU (Gated Recurrent Unit), dalam mengenali dan mempelajari pola-pola kompleks pada data transaksi kartu kredit yang mengandung kasus fraud.
- 2) Mengevaluasi kinerja model ensemble machine learning (Random Forest dan AdaBoost) dibandingkan dengan model ensemble deep learning dalam mendeteksi transaksi kartu kredit yang bersifat fraud.
- 3) Mengimplementasikan metode stacking ensemble dengan Multi-Layer Perceptron (MLP) sebagai meta-learner untuk menggabungkan prediksi dari model deep learning dan machine learning.
- 4) Membandingkan hasil deteksi antara model tunggal dan model stacking ensemble berdasarkan metrik evaluasi akurasi, precision, recall, dan F1-score.
- 5) Memberikan rekomendasi pendekatan model yang paling efektif dan robust untuk deteksi penipuan kartu kredit pada dataset dengan ketidakseimbangan kelas yang tinggi.

1.5. Manfaat Penelitian

- 1) Memberikan kontribusi pada pengembangan ilmu pengetahuan di bidang *credit card fraud detection* dengan mengintegrasikan pendekatan deep learning dan machine learning melalui ensemble learning.
- 2) Menjadi referensi bagi penelitian selanjutnya yang mengkaji kombinasi model berbasis sekuensial dan berbasis pohon keputusan untuk permasalahan klasifikasi pada data yang tidak seimbang.
- 3) Memberikan alternatif solusi bagi industri perbankan dan penyedia layanan pembayaran digital dalam membangun sistem deteksi fraud yang akurat, efisien, dan adaptif.
- 4) Mengurangi potensi kerugian finansial serta meningkatkan kepercayaan masyarakat terhadap sistem pembayaran digital melalui penerapan model deteksi fraud yang lebih robust.

1.6. Sistematika Penulisan

BAB I PENDAHULUAN, Bab ini membahas latar belakang masalah yang menjelaskan urgensi dari *credit card fraud detection* pada era digital, rumusan masalah yang menjadi fokus penelitian, batasan penelitian untuk memperjelas ruang lingkup studi, tujuan penelitian yang ingin dicapai, manfaat teoretis dan praktis yang diharapkan, serta sistematika penulisan yang memberikan gambaran keseluruhan struktur skripsi.

BAB II TINJAUAN PUSTAKA, Bab ini memuat kajian literatur dan dasar teori yang relevan. Kajian literatur menjelaskan penelitian-penelitian terdahulu yang terkait dengan deteksi penipuan kartu kredit menggunakan metode *machine learning* dan *deep learning*, termasuk penerapan *stacking ensemble*. Bagian dasar teori menguraikan konsep dan prinsip yang digunakan, seperti *machine learning*, *deep learning*, *artificial neural network*, *LSTM*, *GRU*, *random forest*, *ensemble learning*, *meta-learner*, dan *multi-layer perceptron (MLP)*, sebagai landasan teoretis penelitian ini.

BAB III METODE PENELITIAN, Bab ini menjelaskan metodologi yang digunakan secara sistematis. Uraian dimulai dengan deskripsi objek penelitian dan dataset, diikuti alur penelitian yang menggambarkan tahapan eksplorasi data, preprocessing, pembagian data, proses pelatihan model, serta evaluasi kinerja. Bab ini juga mencakup arsitektur model *deep learning* (*LSTM* dan *GRU*), algoritma *machine learning* (*Random Forest* dan *AdaBoost*), serta integrasi *stacking ensemble* dengan *MLP* sebagai *meta-learner*. Selain itu, dibahas alat dan bahan yang digunakan dalam penelitian, termasuk Bahasa pemrograman python, library, dan infrastruktur komputasi.

BAB IV HASIL DAN PEMBAHASAN, Bab ini memaparkan hasil eksperimen dan analisis mendalam terhadap performa model. Hasil yang disajikan mencakup eksplorasi dataset, preprocessing, evaluasi model *deep learning* dan *machine learning*, serta perbandingan performa menggunakan metrik akurasi,

presisi, recall, F1-score, AUC-ROC, dan kurva Precision-Recall. Analisis pembahasan menyoroti keunggulan dan keterbatasan setiap model, efektivitas pendekatan *stacking ensemble*, serta implikasi hasil penelitian terhadap pengembangan sistem deteksi penipuan yang lebih akurat dan stabil.

BAB V PENUTUP, berisi kesimpulan dan saran yang dapat peneliti rangkum selama proses penelitian.

