BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan transaksi digital dalam sektor keuangan dan *e-commerce* telah meningkatkan risiko terjadinya *fraud* atau kecurangan pada transaksi [1]. *Fraud detection* menjadi salah satu permasalahan krusial dalam industri keuangan karena berpotensi menimbulkan kerugian finansial yang signifikan serta merusak reputasi institusi [2]. Dalam transaksi keuangan digital, khususnya penggunaan kartu pembayaran dan transaksi berbasis internet telah memberikan kemudahan serta efisiensi bagi pengguna dalam melakukan aktivitas finansial tetapi juga meningkatkan potensi terjadinya *fraud* pada sistem pembayaran modern [2], [3]. Seiring dengan meningkatnya volume dan kompleksitas transaksi digital, sistem deteksi *fraud* dituntut untuk mampu mengidentifikasi pola kecurangan secara cepat dan akurat [3]. Oleh karena itu, diperlukan pendekatan yang tidak hanya mampu mencapai tingkat akurasi tinggi, tetapi juga mampu menangani data dalam skala besar secara efisien [4].

Peningkatan aktivitas pembayaran digital menyebabkan kebutuhan terhadap sistem deteksi *fraud* yang lebih efektif karena transaksi finansial memiliki pola yang semakin kompleks dan sulit diidentifikasi hanya menggunakan metode berbasis aturan konvensional [2], [3]. Kondisi tersebut menunjukkan bahwa *fraud* pada transaksi digital telah menjadi salah satu tantangan penting dalam menjaga keamanan dan keandalan sistem keuangan modern [2], [3]. Penelitian dari Seera et al. menunjukkan bahwa meningkatnya penggunaan *payment card* mendorong kebutuhan terhadap sistem *fraud detection* yang mampu mengenali pola transaksi mencurigakan secara akurat dan efisien [2]. Selain itu, Khalid et al. menjelaskan bahwa *credit card fraud* masih menjadi permasalahan penting karena pendekatan tradisional menghadapi berbagai keterbatasan seperti ketidakseimbangan data, meningkatnya kompleksitas pola *fraud*, serta tantangan dalam menghasilkan

prediksi yang akurat pada transaksi finansial [5]. Permasalahan tersebut menunjukkan bahwa *fraud detection* membutuhkan pendekatan yang mampu mempelajari pola transaksi secara otomatis serta beradaptasi terhadap karakteristik data *fraud* yang kompleks [3], [5].

Dalam konteks dataset transaksi nyata, penelitian Irawan menunjukkan bahwa deteksi *fraud* kartu kredit merupakan permasalahan klasifikasi dengan distribusi kelas yang tidak seimbang karena transaksi *fraud* memiliki jumlah yang jauh lebih sedikit dibandingkan transaksi normal dengan proporsi sebesar 0,17% yang menegaskan bahwa *fraud detection* merupakan masalah *class imbalance* yang sangat kuat [6]. Ketidakseimbangan kelas tersebut dapat menyebabkan model *machine learning* lebih dominan mempelajari pola kelas mayoritas sehingga kemampuan mendeteksi transaksi *fraud* sebagai kelas minoritas menjadi kurang optimal [4], [7]. Oleh karena itu, berbagai penelitian menerapkan metode *handling imbalance data* seperti teknik *resampling* dan pendekatan *ensemble learning* untuk meningkatkan kemampuan model dalam mengenali transaksi *fraud* [4], [7].

Kebutuhan akan sistem yang efisien tersebut semakin penting mengingat karakteristik dataset transaksi keuangan yang umumnya berukuran besar memiliki kombinasi fitur numerik dan kategorikal, serta menunjukkan ketidakseimbangan kelas (*imbalanced data*), di mana jumlah transaksi normal jauh lebih banyak dibandingkan transaksi *fraud* [5]. Kondisi ini menyebabkan model *machine learning* cenderung *bias* terhadap kelas mayoritas jika tidak ditangani dengan baik [7]. Maka, diperlukan pendekatan yang mampu mengelola data dalam skala besar sekaligus mempertahankan performa model dalam kondisi distribusi data yang tidak seimbang [8].

Dalam menangani tantangan tersebut, dilakukan integrasi dengan penggunaan algoritma *machine learning* yang sesuai untuk menangani karakteristik data transaksi [9]. Dalam hal ini, algoritma berbasis *ensemble* seperti Gradient Boosted Tree (GBT) dipilih karena memiliki kemampuan yang baik dalam menangkap hubungan non-linear antar fitur serta meningkatkan akurasi prediksi dibandingkan

model berbasis pohon tunggal [10], [11]. Selain itu, model dengan performa tinggi sering kali memiliki kompleksitas yang lebih besar sehingga diperlukan pendekatan tambahan untuk meningkatkan interpretabilitas model [12].

Kebutuhan akan interpretabilitas ini menjadi penting karena hasil prediksi dalam sistem *fraud detection* sering kali digunakan sebagai dasar pengambilan keputusan [13]. Oleh karena itu, penelitian ini mengintegrasikan pendekatan *Explainable Artificial Intelligence* (XAI) menggunakan SHAP (*Shapley Additive Explanations*) untuk memberikan penjelasan terhadap hasil prediksi model melalui analisis kontribusi fitur [14]. Dengan adanya SHAP, model tidak hanya menghasilkan prediksi, tetapi juga memberikan pemahaman yang lebih transparan mengenai faktor-faktor yang mempengaruhi keputusan model, sehingga meningkatkan kepercayaan terhadap sistem yang dikembangkan [15], [16].

Selain pendekatan berbasis model utama dan interpretabilitas, penelitian ini juga mengeksplorasi pendekatan alternatif untuk menangkap pola *fraud* yang lebih kompleks. Salah satu pendekatan yang digunakan adalah *Graph Neural Network* (GNN) yang mampu merepresentasikan hubungan antar entitas seperti transaksi dan *merchant* dalam bentuk struktur *graph* [17]. Pendekatan ini memungkinkan model untuk menangkap pola relasional yang tidak dapat diidentifikasi oleh model berbasis tabular tradisional [18], [19]. Di sisi lain, penelitian ini juga mengimplementasikan konsep *Federated Learning* (FL) sebagai simulasi pembelajaran terdistribusi, di mana model dilatih pada beberapa *subset* data secara terpisah sebelum dilakukan agregasi hasil model [13], [20]. Penelitian terbaru juga mengeksplorasi penggunaan *Federated Learning* untuk mengatasi keterbatasan berbagi data transaksi finansial yang bersifat sensitif antar institusi [20]. Abdul Salam et al. menunjukkan bahwa *Federated Learning* dapat diterapkan pada *credit card fraud detection* dengan menggabungkan pembelajaran terdistribusi dan teknik penanganan ketidakseimbangan data [21].

Meskipun berbagai pendekatan seperti *Graph Neural Network* (GNN) dan *Federated Learning* (FL) menawarkan kemampuan dalam deteksi *fraud*, implementasinya secara umum melibatkan kompleksitas arsitektur dan kebutuhan komputasi yang lebih tinggi [22]. Oleh karena itu, diperlukan pemilihan model yang tidak hanya memiliki performa klasifikasi yang baik, tetapi juga dapat diimplementasikan dalam sistem *deployment* [23]. Dalam penelitian ini, model GBT dipilih sebagai model utama untuk *deployment* karena memiliki keseimbangan antara performa dan efisiensi [24].

Integrasi antara model dan sistem *deployment* kemudian diwujudkan melalui pengembangan aplikasi berbasis Streamlit yang memungkinkan pengguna melakukan prediksi *fraud* secara *near real-time* [25]. Dalam sistem ini, data *input* pengguna akan diproses menggunakan *pipeline* yang sama seperti pada tahap pelatihan model, sehingga memastikan konsistensi antara eksperimen dan implementasi [26]. Dengan demikian, penelitian ini tidak hanya berfokus pada pengembangan model, tetapi juga pada implementasi sistem yang dapat digunakan secara praktis [27].

Penelitian terkait deteksi *fraud* pada transaksi keuangan digital umumnya masih berfokus pada peningkatan performa klasifikasi tanpa memberikan perhatian yang cukup terhadap interpretabilitas model dan analisis pola perilaku transaksi *fraud* [28]. Selain itu, beberapa penelitian sebelumnya masih memiliki keterbatasan dalam pengolahan data berskala besar serta belum banyak mengeksplorasi pendekatan alternatif yang mampu menangkap hubungan relasional antar entitas maupun aspek privasi data dalam proses pembelajaran model [29], [30]. Kondisi tersebut menyebabkan sistem deteksi *fraud* sering kali sulit diinterpretasikan dan kurang optimal untuk diterapkan pada lingkungan transaksi digital yang kompleks dan dinamis [31]. Oleh karena itu, penelitian ini dilakukan untuk mengembangkan model deteksi *fraud* yang tidak hanya memiliki performa klasifikasi yang baik, tetapi juga mampu memberikan interpretasi terhadap hasil prediksi, mendukung pengolahan data berskala besar, serta mengeksplorasi pendekatan tambahan seperti

Graph Neural Network dan *Federated Learning* dalam analisis *fraud* pada transaksi keuangan digital.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk mengembangkan dan mengevaluasi sistem deteksi *fraud* transaksi digital berbasis Big Data menggunakan *Gradient Boosted Tree* (GBT) yang didukung oleh *Explainable Artificial Intelligence* (XAI) melalui metode SHAP. Penelitian ini juga mengeksplorasi pendekatan alternatif seperti *Graph Neural Network* (GNN) dan *Federated Learning* (FL) untuk menganalisis potensi pengembangan sistem deteksi *fraud* yang lebih kompleks dan *privacy-preserving*. Selain itu, penelitian ini berfokus pada pengembangan sistem *fraud prediction* yang mampu mendeteksi transaksi baru secara lebih interpretatif dan *scalable* untuk diimplementasikan dalam lingkungan *deployment*. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan sistem deteksi *fraud* yang tidak hanya memiliki performa klasifikasi yang baik, tetapi juga mendukung aspek interpretabilitas, skalabilitas, dan kesiapan implementasi pada sistem nyata.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijabarkan, maka rumusan masalah dalam penelitian ini adalah:

1. Bagaimana performa model Gradient Boosted Tree (GBT) dalam mendeteksi transaksi *fraud* pada *dataset* berskala besar dan tidak seimbang?
2. Bagaimana kontribusi pendekatan Explainable Artificial Intelligence (XAI) menggunakan metode SHAP dalam meningkatkan interpretabilitas model *fraud detection*?
3. Bagaimana hasil eksperimen komparatif *Graph Neural Network*s (GNN) dan *Federated Learning* (FL) dibandingkan GBT, serta potensi penerapan keduanya dalam skenario *fraud detection* yang tidak ditangani secara optimal oleh model tabular seperti GBT?

1.3 Batasan Masalah

Agar penelitian lebih terfokus, maka ditetapkan batasan masalah sebagai berikut:

1. *Dataset* yang digunakan merupakan *dataset* transaksi keuangan sintetis dengan karakteristik skala besar dan *imbalanced* yang bersumber dari Kaggle.
2. Model utama yang digunakan adalah Gradient Boosted Tree (GBT) sebagai algoritma klasifikasi berbasis *ensemble*.
3. *Federated Learning* (FL) digunakan sebagai simulasi pembelajaran terdistribusi untuk mengevaluasi dampak pembatasan fitur tanpa mengimplementasikan protokol komunikasi klien-server secara nyata.
4. Pendekatan tambahan yang digunakan dalam penelitian ini meliputi:
    a. *Explainable AI* (SHAP) untuk interpretabilitas model
    b. *Graph Neural Network* (GNN) untuk analisis berbasis relasi
    c. *Federated Learning* (FL) untuk simulasi pembelajaran terdistribusi
5. Evaluasi model dilakukan menggunakan metrik:
    a. AUC-ROC
    b. Precision
    c. Recall
    d. F1-score
    e. Accuracy
6. Implementasi *deployment* dilakukan menggunakan aplikasi berbasis Streamlit untuk simulasi prediksi *fraud* pada transaksi baru secara interaktif.
7. Penelitian ini tidak membahas integrasi sistem hingga *production-level* secara penuh, melainkan terbatas pada simulasi *deployment*.

1.4 Tujuan dan Manfaat Penelitian

1.4.1 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Menganalisis performa model Gradient Boosted Tree (GBT) dalam mendeteksi transaksi *fraud* pada *dataset* berskala besar.

2. Mengimplementasikan dan mengevaluasi pendekatan *Explainable AI* (SHAP) untuk meningkatkan transparansi dan interpretabilitas model.
3. Mengeksplorasi potensi pendekatan alternatif seperti *Graph Neural Network* (GNN) dan *Federated Learning* (FL) dalam mendukung analisis *fraud detection*.

1.4.2 Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1. Memberikan kontribusi dalam pengembangan sistem *fraud detection* berbasis Big Data.
2. Menambah referensi akademik terkait penggunaan Gradient Boosted Tree dalam lingkungan komputasi terdistribusi.
3. Menunjukkan pentingnya *Explainable AI* (SHAP) dalam meningkatkan transparansi model *machine learning* pada industri keuangan.
4. Memberikan wawasan mengenai penerapan pendekatan alternatif seperti *Graph Neural Network* (GNN) dan *Federated Learning* (FL) dalam analisis *fraud detection*.
5. Menyediakan contoh implementasi sistem deteksi *fraud* berbasis web menggunakan Streamlit yang mendukung simulasi prediksi transaksi baru secara interaktif.

1.5 Kontribusi Penelitian

Berdasarkan tinjauan terhadap penelitian terdahulu pada tabel 2.1, terdapat beberapa celah yang belum ditangani secara bersamaan dalam satu kerangka kerja terintegrasi. Sebagian besar penelitian yang ada berfokus pada satu pendekatan tunggal baik peningkatan performa klasifikasi [6], [32], interpretabilitas model [13], [33], analisis relasional berbasis graf [34], [35], maupun privasi melalui *Federated Learning* [36] tanpa mengintegrasikan seluruh aspek tersebut dalam satu *pipeline* yang juga mencakup validasi Big Data dan implementasi sistem yang dapat digunakan secara langsung. Selain itu, penelitian yang membandingkan GBT, GNN, dan FL secara kuantitatif dalam satu eksperimen terkontrol pada dataset skala

jutaan baris dengan justifikasi pemilihan model yang berbasis karakteristik data masih sangat terbatas. Berdasarkan celah tersebut, kontribusi utama penelitian ini adalah sebagai berikut:

1. **Framework Analisis Komparatif Terintegrasi Berbasis Big Data**

Berbeda dari penelitian sebelumnya yang umumnya mengevaluasi satu metode secara terisolasi, penelitian ini menyatukan GBT, SHAP, GNN, dan FL dalam satu *pipeline* eksperimen yang diimplementasikan menggunakan PySpark pada dataset 7,4 juta baris. Kontribusi ini mengisi celah dari penelitian seperti Irawan (2025) dan Alrasheedi (2025) [6], [32] yang menggunakan *ensemble method* namun tidak mengeksplorasi pendekatan relasional maupun terdistribusi, serta dari Huang (2025) dan Du (2025) [34], [35] yang menggunakan GNN namun tidak menyertakan perbandingan dengan model tabular maupun analisis interpretabilitas. Dengan *framework* ini, penelitian memberikan panduan berbasis bukti empiris mengenai kondisi data seperti apa yang paling sesuai untuk masing-masing pendekatan.

2. **Sistem Deteksi Fraud dengan Interpretabilitas Terintegrasi pada Antarmuka Pengguna**

Penelitian ini mengembangkan prototipe FraudShield yang mengintegrasikan SHAP langsung ke dalam antarmuka pengguna, sehingga setiap prediksi disertai narasi penjelasan yang dapat dipahami oleh analis *fraud* tanpa latar belakang teknis. Hal ini membedakan penelitian ini dari Aljunaid dkk. (2025) [13] dan Muksalmina dkk. (2025) [33] yang menggunakan SHAP hanya pada tahap analisis model, bukan sebagai bagian dari sistem yang dapat dioperasikan secara langsung oleh pengguna akhir.

3. **Analisis Kuantitatif Dampak Keterbatasan Fitur pada *Federated Learning***

Melalui perbandingan skenario FL dengan 18 fitur lengkap dan 5 fitur parsial, penelitian ini memberikan pengukuran presisi terhadap penurunan performa (selisih AUC 0,0393, selisih F1 0,0600) akibat keterbatasan berbagi fitur antar institusi. Kontribusi ini lebih spesifik dibandingkan Alam (2025) [36] yang mengeksplorasi FL dengan *blockchain* namun tidak mengukur dampak keterbatasan fitur secara

kuantitatif, maupun Aljunaid dkk. (2025) [13] yang mengintegrasikan FL dengan XAI namun tidak mensimulasikan skenario keterbatasan data antar klien. Temuan ini memberikan referensi empiris bagi lembaga keuangan yang sedang mempertimbangkan adopsi FL dalam kondisi regulasi privasi yang membatasi berbagi fitur sensitif.

1.6 Sistematika Penulisan

Sistematika penulisan dalam penelitian ini disusun sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi latar belakang, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, serta sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini membahas teori-teori yang mendukung penelitian, meliputi konsep *fraud detection*, *machine learning* untuk klasifikasi, Gradient Boosted Tree (GBT), Explainable Artificial Intelligence (XAI) dengan SHAP, *Graph Neural Network* (GNN), *Federated Learning* (FL), serta konsep Big Data.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan tahapan penelitian yang meliputi *data ingestion*, *data understanding*, *data preprocessing*, *feature engineering*, *feature encoding*, pembagian data *training* dan *testing*, pembangunan model menggunakan Gradient Boosted Tree (GBT), serta implementasi pendekatan tambahan seperti SHAP untuk interpretabilitas, GNN untuk analisis relasional, dan *Federated Learning* untuk simulasi pembelajaran terdistribusi. Selain itu, bab ini juga menjelaskan metode evaluasi model serta integrasi *pipeline* ke dalam sistem *deployment* berbasis Streamlit.

BAB IV ANALISIS DAN HASIL PENELITIAN

Bab ini menyajikan hasil eksperimen dan evaluasi performa model menggunakan metrik seperti AUC, Precision, Recall, F1-score, dan Accuracy. Selain itu,

dilakukan analisis terhadap hasil model utama serta eksplorasi pendekatan alternatif seperti GNN dan *Federated Learning*, serta interpretasi model menggunakan SHAP untuk memahami kontribusi fitur dalam prediksi *fraud*.

BAB V SIMPULAN DAN SARAN

Bab ini berisi kesimpulan yang diperoleh dari hasil penelitian serta saran untuk pengembangan penelitian selanjutnya termasuk potensi peningkatan model, penggunaan data yang lebih kompleks, serta implementasi sistem dalam lingkungan yang lebih luas.