BAB I
PENDAHULUAN

1.1. Latar Belakang

Dalam perkembangan dunia saat ini yang serba cepat, revolusi *society* 5.0 membawa masyarakat menuju kehidupan *digitalisasi* yang tidak dapat dihindari terutama pada sektor jasa keuangan. Kemudahan dan kecepatan yang ditawarkan oleh adanya teknologi finansial (*fintech*) telah mendorong adopsi luas oleh masyarakat [1]. Metode pembayaran tradisional yaitu menggunakan uang tunai, kini telah beralih menggunakan pembayaran elektronik dan *digital*. Perubahan ini tidak hanya memudahkan konsumen dalam melakukan transaksi pembayaran tetapi juga meningkatkan efisiensi operasional bagi para pelaku usaha dan institusi keuangan. Dalam satu dekade terakhir, berbagai instrumen pembayaran semakin beragam, dimana ditandai dengan munculnya uang elektronik yang memiliki teknologi berbasis kartu (*chip-based*) dan server (*server-based*)[2]. Namun, perkembangan instrumen ini juga berpotensi menimbulkan risiko ekonomi, seperti penggelembungan nilai (*bubble*), pencucian uang, hingga penyalahgunaan kepentingan untuk pendanaan terorisme, yang pada akhirnya dapat mengganggu stabilitas sistem keuangan dan merugikan masyarakat. Fenomena perubahan ini dibuktikan oleh data yang mengungkapkan perkembangan jumlah instrumen pembayaran elektronik berupa kartu, serta fluktuasi dalam volume dan nilai transaksinya di Indonesia.

Bank Indonesia merilis data mengenai Statistik Sistem Pembayaran dan Infrastruktur Pasar Keuangan Indonesia (SPIP)[3], jumlah kartu atau instrumen untuk uang elektronik terus meningkat. Data terakhir, yaitu Mei 2025 menunjukkan jumlah kartu/instrumen untuk uang elektronik mencapai 975,05 juta unit sedangkan tahun lalu 861,43 juta unit. Nilai transaksi menggunakan uang elektronik mengalami kenaikan yang signifikan, yaitu Rp269,436 miliar per Mei 2025 dengan nilai transaksi Mei 2024 sejumlah Rp204,240 miliar. Sedangkan volume transaksi untuk uang elektronik juga mengalami peningkatan dimana pada per Mei 2025 volume transaksi mencapai angka 2.624.455 ribu transaksi dan Mei 2024 sejumlah 1.823.135 ribu transaksi.

Di tengah meningkatnya ancaman kejahatan siber dan modus penipuan *digital* (*phishing*), sistem deteksi *fraud* menjadi garda terdepan dalam melindungi transaksi keuangan. Menurut siaran pers yang dikeluarkan oleh OJK [4], sejak awal beroperasi hingga hingga 23 Maret 2025, Indonesia *Anti-Scam Centre* (IASC) telah menerima sebanyak 74.243 laporan terkait penipuan. Dari laporan tersebut, terdapat 78.041 rekening yang terindikasi terlibat, dan 33.857 rekening di antaranya sudah berhasil diblokir. Total kerugian yang dialami para korban mencapai Rp1,4 triliun, dengan Rp133,2 miliar dana berhasil dibekukan. Data tersebut menunjukkan bahwa upaya deteksi dan pencegahan *fraud* sangat mendesak bagi industri keuangan. Dengan adanya sistem pendeteksian terhadap transaksi pembayaran, risiko finansial yang memiliki dampak negatif bagi perusahaan dapat diminimalisirkan. Selain itu, sistem ini juga dapat membantu menjaga reputasi perusahaan di mata klien perbankan dan membantu menjaga kepercayaan konsumen, dengan memastikan transaksi berjalan dengan aman serta mematuhi regulasi serta standar keamanan yang berlaku.

PT. XYZ masih menggunakan pendekatan *static rule-based system* dalam mengidentifikasi indikasi *fraud* pada transaksi pembayaran. Sistem ini bekerja dengan mengandalkan serangkaian aturan yang telah ditentukan sebelumnya untuk mendeteksi pola transaksi yang mencurigakan, seperti transaksi dalam jumlah besar dalam rentang waktu yang singkat, atau dua transaksi yang terjadi di lokasi geografis yang berjauhan dalam waktu berdekatan. Meskipun metode ini cukup efektif pada tahap awal implementasi, ia memiliki keterbatasan dalam menghadapi pola transaksi yang semakin kompleks dan dinamis. Tantanga lain yaitu serta sulit beradaptasi terhadap pola penipuan baru yang tidak tercakup dalam aturan yang sudah ada. Untuk mengatasi keterbatasan tersebut, PT. XYZ perlu mempertimbangkan penerapan pendekatan yang lebih dinamis, adaptif, dan efisien, salah satunya dengan memanfaatkan *Machine Learning* (ML). Pendekatan ini memungkinkan sistem deteksi *fraud* menjadi lebih fleksibel karena mampu belajar dari data transaksi yang terus berkembang dan menyesuaikan aturan secara otomatis. Dengan demikian, sistem dapat memperbarui deteksi secara mandiri, meningkatkan akurasi, dan merespons

potensi *fraud* dengan lebih cepat tanpa bergantung sepenuhnya pada intervensi manual.

Salah satu pendekatan yang dapat diterapkan adalah *Machine Learning* (ML), yang memiliki kemampuan untuk mempelajari pola dari data transaksi historis secara otomatis. Sistem berbasis ML tidak hanya mampu mendeteksi pola transaksi yang telah dikenali sebelumnya, tetapi juga dapat mengidentifikasi pola-pola baru yang belum tertangkap oleh aturan statis. Hal ini memungkinkan sistem deteksi *fraud* menjadi lebih fleksibel, akurat, dan responsif terhadap dinamika transaksi. Namun, tantangan dari penggunaan ML terletak pada sifatnya yang sering kali menyerupai *black box*, di mana proses pengambilan keputusan oleh model sulit dipahami karena tidak memberikan penjelasan eksplisit terhadap alasan di balik prediksinya. Untuk mengatasi hal tersebut, PT. XYZ dapat mengintegrasikan ML dengan *Explainable Artificial Intelligence* (XAI), yaitu pendekatan dalam kecerdasan buatan yang dirancang untuk menghasilkan prediksi yang dapat dijelaskan secara manusiawi. Teknologi ini memungkinkan sistem menjelaskan alasan di balik keputusan yang diambil, seperti mengapa suatu transaksi diklasifikasikan sebagai *fraud*. Dengan kombinasi ML dan XAI, sistem tidak hanya menjadi lebih adaptif dan akurat, tetapi juga lebih transparan dan dapat dipertanggungjawabkan. Sehingga PT. XYZ mampu meningkatkan kepercayaan dari mitra bank maupun nasabah.

Sejumlah studi terdahulu telah dilakukan untuk mengevaluasi efektivitas berbagai algoritma *Machine Learning* dalam mendeteksi transaksi *Fraud*, dengan pendekatan dan metode yang beragam. Penelitian yang dilakukan oleh Mehvish dan Ravinder Pal Singh membandingkan dua algoritma *Machine Learning*, yaitu *Random Forest (RF)* dan *Extreme Learning Machine (ELM)*, untuk mendeteksi penipuan kartu kredit. Penelitian ini melalui tahapan *data collecting*, *data preprocessing* (meliputi *data cleaning*, *data normalization*, dan *feature engineering*), pembagian *dataset* menjadi *training* dan *testing*, serta evaluasi model. Hasil penelitian menunjukkan bahwa algoritma ELM memiliki akurasi lebih tinggi, yaitu 99,8%, dibandingkan dengan RF yang mencapai akurasi 98,56%. Hal ini membuktikan bahwa ELM lebih efektif dalam mendeteksi aktivitas penipuan pada transaksi kartu kredit [5].

Dengan topik yang sama penelitian dilakukan oleh Rahmatullah, dkk membahas tentang pengujian beberapa metode *Machine Learning,* kemudian dioptimalkan dengan fungsi SMOTE untuk mengklasifikasikan transaksi penipuan (*fraud detection*). Hasil dari penelitian ini adalah fungsi SMOTE berhasil meningkatkan nilai *recall* dengan menggunakan model terbaik, yaitu Gradient Boosting dengan SMOTE sebesar 92%. 2 model lainnya, yaitu XGBoost dan AdaBoost, menghasilkan nilai *recall* sebesar 91% untuk keduanya, hanya perbedaan 1% dari model terbaik yang dijelaskan sebelumnya[6].

Berbeda dengan penelitian sebelumnya, Rejna Azeez N., dkk. mengarahkan fokus pada pengembangan *Network Intrusion Detection System (NIDS)* dengan menerapkan *Explainable Artificial Intelligence (XAI)* menggunakan *Local Interpretable Model-agnostic Explainations* (LIME). Penelitian ini membandingkan kinerja beberapa model *Machine Learning*, seperti *Random Forest*, *Linear Regression*, *Decision Tree*, *LGBM*, dan *Ensemble Learning*. Hasil penelitian menunjukkan bahwa model LGBM memiliki akurasi terbaik sebesar 94%, diikuti oleh *Linear Regression* (88%), *Random Forest* (87%), dan *Decision Tree* (83%). Penelitian ini juga menekankan pentingnya penerapan XAI untuk memberikan penjelasan yang mudah dipahami terkait prediksi model, sehingga meningkatkan kepercayaan pengguna terhadap sistem[7]

Dari penelitian sebelumnya yang membahas tentang analisis sistem deteksi *fraud* pada transaksi keuangan dan kartu kredit menggunakan algoritma *Machine Learning* dan implementasi *imbalancing data* telah memberikan kontribusi signifikan dalam bidangnya[8]. Oleh karena itu, penelitian ini memberikan keterbaruan dengan menggunakan data yang berasal dari PT. XYZ sebagai penyedia layanan transaksi keuangan di Indonesia. Metode *Machine Learning* yang akan diterapkan adalah *Extreme Learning Machine* yang dikombinasikan dengan beberapa metode *resampling* untuk menangani ketidakseimbangan data *fraud* yang umum ditemui pada *dataset* transaksi pembayaran. Karena deteksi *fraud* termasuk dalam kategori klasifikasi biner, pendekatan ini dinilai sesuai untuk mengidentifikasi transaksi secara otomatis berdasarkan pola dari data sebelumnya, meskipun terdapat ketidakseimbangan

kelas. *Extreme Learning Machine* dipilih sebagai algoritma utama dalam panelitian ini karena ELM memiliki kemampuan untuk melatih model secara cepat dengan performa yang kompetitis dibandingkan dengan metode *Machine Learning* lainnya. ELM bekerja berdasarkan arsitektur *Single Layer Feedforward Neural Network* (SLFN), dimana bobot dan biar diatur secara acak, sementara bobot *output* dihitung secara analitik. Selain itu, pada penelitian ini juga akan dilakukan analisis sistem deteksi *fraud* yang mengimplementasikan *Explainable Artificial Intelligence* (XAI), dengan metode *Local Interpretable Model-agnostic Explanations* (LIME). Dengan adanya keterbaruan analisis menggunakan metode XAI diharapkan mampu memberikan transparansi dan interpretabilitas yang lebih baik dalam mendeteksi *fraud.* Sehingga PT. XYZ dapat meningkatkan kredibilitas layanannya, serta membangun kepercayaan yang lebih kuat dari bank dan nasabah.

1.2. Rumusan Masalah

Rumusan masalah yang dapat diidentifikasi dari penjelasan latar belakang, sebagai berikut:

1. Bagaimana data transaksi pembayaran *online* di PT. XYZ dapat dimanfaatkan untuk penerapan algoritma *Extreme Learning Machine* dalam mendeteksi *fraud*?
2. Bagaimana implementasi algoritma *Extreme Learning Machine* serta peran *Explainable Artificial Intelligence* (XAI) dalam mengidentifikasi dan menjelaskan penyebab *fraud* pada transaksi pembayaran *online*?
3. Bagaimana performa sistem deteksi *fraud* yang dibangun dengan algoritma *Extreme Learning Machine* dievaluasi menggunakan metrik performa yang sesuai?
4. Bagaimana *interface* sistem deteksi *fraud* pembayaran *online* yang mengintegrasikan *Extreme Learning Machine* dan *Explainable Artificial Intelligence* (XAI) dapat membantu penyedia layanan untuk menganalisis dan memantau transaksi pembayaran yang mencurigakan?

1.3. Batasan Masalah

Batasan masalah yang ditetapkan pada penelitian ini diantaranya:

1. Penelitian ini menggunakan data transaksi pembayaran *online* yang tersedia pada PT. XYZ.
2. Penelitian ini memanfaatkan metode XAI *Local Interpretable Model-Agnostic Explanation* (LIME) sebagai pendekatan untuk memberikan interpretasi pada hasil prediksi model.
3. Sistem yang dibangun hanya digunakan untuk mendeteksi transaksi mencurigakan berdasarkan data historis, tidak akan membahas aspek mitigasi atau tindakan lebih lanjut yang harus diambil oleh operator setelah terdeteksi *fraud*
4. Pengujian sistem deteksi *fraud* akan dilakukan pada data historis yang disediakan oleh PT. XYZ dalam jangka waktu tertentu, tidak mencakup pengujian secara langsung atau *real-time*.

1.4. Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Memanfaatkan data transaksi pembayaran *online* di PT. XYZ menggunakan algoritma *Extreme Learning Machine* dalam mendeteksi *fraud.*
2. Mengimplementasikan algoritma *Extreme Learning Machine* serta peran *Explainable Artificial Intelligence* (XAI) dalam mengidentifikasi dan menjelaskan penyebab *fraud* pada transaksi pembayaran *online.*
3. Mengevaluasi performa sistem deteksi *fraud* yang dibangun dengan algoritma *Extreme Learning Machine* menggunakan metrik evaluasi yang sesuai.
4. Mengetahui *interface* sistem deteksi *fraud* pembayaran *online* yang mengintegrasikan *Extreme Learning Machine* dan *Explainable Artificial Intelligence* (XAI) dapat membantu penyedia layanan untuk menganalisis dan memantau transaksi pembayaran yang mencurigakan

1.5. Manfaat Penelitian

Penelitian mengenai Analisis Sistem Deteksi *fraud* Menggunakan *Machine Learning* dan *Explainable Artificial Intelligence* diharapkan mampu memberikan manfaat dari berbagai sisi, seperti sisi akademis, praktis, maupun pengembangan ilmu pengetahuan di bidang terkait, seperti berikut:

1. Mengetahui pemanfaatan data transaksi pembayaran *online* saat diterapkan menggunakan algoritma *Machine Learning* untuk mendeteksi adanya *fraud*
2. Mengetahui pengimplementasian algoritma *Machine Learning* dan diintegrasikan dengan *Explainable Artificial Intelligence* untuk mendeteksi dan menjelaskan penyebab adanya *fraud* pada transaksi pembayaran *online*
3. Mengetahui evaluasi performa dari sistem deteksi *fraud* yang dibangun dengan algoritma *Extreme Learning Machine* menggunakan metrik evaluasi yang sesuai.
4. Memberikan alat analisis yang dapat melakukan deteksi *fraud* transaksi pembayaran *online* secara akurat dan efisien.

Halaman ini sengaja dikosongkan