Business Requirement Document (BRD)

Perbandingan Algorithma XGBoost–SMOTE dan Random Forest–SMOTE untuk Deteksi Fraud Transaksi Kartu Kredit Berdasarkan Standar POJK No. 11/POJK.03/2022.

Disusun oleh : Putri Agisnadiansyah
NIM : 20220801330

---

1. Introduction

Dokumen Business Requirement Document (BRD) ini menjabarkan rancangan sistem, kebutuhan fungsional, dan aspek teknis dalam penelitian berjudul: "Perbandingan Algorithma XGBoost-SMOTE dan Random Forest-SMOTE untuk Deteksi Fraud Transaksi Kartu Kredit Berdasarkan Standar POJK No. 11/POJK.03/2022."

Penelitian ini difokuskan pada pengembangan sistem deteksi penipuan (*fraud detection system*) berbasis machine learning, yang mampu mengenali pola transaksi kartu kredit mencurigakan secara akurat, efisien, dan sesuai regulasi perbankan Indonesia. Fokus utama adalah membandingkan performa dua algoritma pembelajaran mesin XGBoost dan Random Forest yang dikombinasikan dengan teknik SMOTE (Synthetic Minority Oversampling Technique) untuk mengatasi masalah ketidakseimbangan data (*imbalanced dataset*) yang umum pada kasus fraud.

Pipeline sistem akan dibangun secara end-to-end, meliputi tahapan:

1. **Data Acquisition** – Pengumpulan dan pemrosesan awal dataset transaksi kartu kredit yang telah dilabeli (fraud dan non-fraud).
2. **Data Preprocessing** – Pembersihan data, encoding, normalisasi, dan deteksi *outlier*.
3. **Data Balancing (SMOTE)** – Oversampling kelas minoritas untuk menyeimbangkan proporsi data.
4. **Model Training (XGBoost & Random Forest)** – Pelatihan dua model pembelajaran mesin dengan parameter teroptimasi.
5. **Model Evaluation** – Pengukuran performa menggunakan metrik seperti Recall, Precision, F1-Score, AUC-ROC, dan False Positive Rate.
6. **Compliance Analysis** – Evaluasi kesesuaian hasil model terhadap standar regulasi POJK No. 11/POJK.03/2022.
7. **Explainable AI (XAI)** – Analisis interpretabilitas model menggunakan SHAP untuk menjelaskan alasan di balik setiap prediksi.

Sistem ini dirancang tidak hanya untuk menunjukkan model mana yang paling akurat, tetapi juga mana yang paling sesuai untuk diterapkan dalam sistem perbankan Indonesia berdasarkan aspek kepatuhan, keamanan, dan interpretabilitas.

Penelitian ini diimplementasikan menggunakan bahasa Python, dengan pustaka utama:

- **Scikit-learn** – untuk preprocessing dan evaluasi,
- **Imbalanced-learn** – untuk penerapan SMOTE,
- **XGBoost** dan **RandomForestClassifier** – untuk pelatihan model,
- **SHAP/LIME** – untuk analisis interpretabilitas model,
- **Matplotlib dan Plotly** – untuk visualisasi hasil analisis.

2. Latar Belakang dan Justifikasi Penelitian

2.1 Konteks Penelitian

Transaksi kartu kredit merupakan salah satu aktivitas keuangan dengan volume data yang sangat besar dan risiko penipuan (*fraud*) yang tinggi. Dalam ekosistem perbankan modern, peningkatan jumlah transaksi digital tanpa peningkatan sistem keamanan yang sepadan dapat menimbulkan potensi kerugian finansial signifikan.

Sistem deteksi penipuan tradisional yang berbasis aturan (*rule-based system*) sering kali gagal mengenali pola penipuan baru karena tidak mampu menyesuaikan diri terhadap perubahan perilaku pelaku kejahatan finansial. Oleh sebab itu, pendekatan berbasis machine learning menjadi solusi alternatif karena dapat mempelajari pola transaksi dari data historis dan mengidentifikasi anomali secara adaptif.

Namun, salah satu tantangan utama dalam deteksi penipuan adalah ketidakseimbangan data (imbalanced dataset) — di mana proporsi transaksi normal dapat mencapai lebih dari 99% dibandingkan transaksi fraud yang sangat sedikit. Kondisi ini menyebabkan model *machine learning* bias terhadap kelas mayoritas dan cenderung mengabaikan kasus penipuan (false negative tinggi).

Untuk mengatasi tantangan tersebut, penelitian ini mengusulkan dua kombinasi algoritma utama yang menggunakan pendekatan SMOTE (Synthetic Minority Oversampling Technique):

1. **XGBoost–SMOTE** – Menggabungkan XGBoost (Extreme Gradient Boosting) dengan SMOTE untuk menghasilkan model deteksi fraud yang kuat dan mampu menangkap pola kompleks secara non-linear.
2. **Random Forest–SMOTE** – Menggabungkan Random Forest dengan SMOTE untuk meningkatkan sensitivitas terhadap kelas minoritas dan menjaga stabilitas model terhadap variasi data.

Kedua pendekatan ini akan dievaluasi secara komparatif untuk menilai performa teknis (Recall, F1-Score, False Positive Rate) serta kepatuhan terhadap standar manajemen risiko TI sebagaimana diatur dalam POJK No. 11/POJK.03/2022.

2.2 Permasalahan Teknis Utama

1. **Distribusi data transaksi sangat tidak seimbang**, dengan rasio fraud < 1% dari total transaksi.

2. **Model konvensional (tanpa balancing)** menghasilkan bias terhadap kelas mayoritas, mengurangi kemampuan deteksi fraud.
3. **Parameter model** (seperti learning rate, n_estimators, max_depth) sering kali tidak dioptimalkan, menyebabkan performa suboptimal.
4. **Ketiadaan analisis interpretabilitas model**, sehingga hasil prediksi sulit dijelaskan kepada pihak regulator dan auditor.
5. **Belum adanya framework evaluasi gabungan** antara kinerja teknis dan kepatuhan regulasi perbankan.

2.3 Solusi Teknis yang Diusulkan

Penelitian ini mengusulkan pembangunan sistem end-to-end comparative machine learning pipeline, yang meliputi tahapan utama berikut:

Tahapan Teknis	**Deskripsi Implementasi**
Preprocessing Module	Pembersihan data, normalisasi, encoding, dan deteksi *outlier*.
Balancing Module (SMOTE Engine)	Oversampling pada kelas minoritas menggunakan SMOTE dengan parameter *k_neighbors = 5*.
Model Training Module (XGBoost & Random Forest)	Pelatihan dua model dengan teknik *cross-validation* dan *hyperparameter tuning*.
Evaluation Module	Perbandingan kinerja kedua model menggunakan metrik: Recall, Precision, F1-Score, AUC-ROC, dan False Positive Rate.
Compliance Analysis Module	Penilaian terhadap kepatuhan model berdasarkan prinsip keamanan dan transparansi POJK No. 11/POJK.03/2022.
Interpretability Module (XAI)	Analisis kontribusi fitur menggunakan SHAP untuk mendukung transparansi hasil prediksi.

Pipeline ini memastikan proses penelitian dilakukan secara sistematis, terukur, dan dapat direproduksi untuk keperluan audit maupun pengujian ulang di masa depan.

2.4 Keunggulan Teknis Penelitian

- **Kinerja Tinggi:** Kombinasi SMOTE dengan algoritma berbasis ensemble meningkatkan sensitivitas terhadap transaksi fraud.
- **Stabilitas Model:** Random Forest–SMOTE cenderung lebih stabil terhadap *overfitting* dibanding metode tunggal.

- **Efisiensi Komputasi:** XGBoost mendukung paralelisasi GPU untuk mempercepat waktu pelatihan.
- **Interpretabilitas Tinggi:** Integrasi SHAP mendukung *Explainable AI* untuk keperluan audit dan kepatuhan regulasi.
- **Kepatuhan Regulasi:** Desain sistem diselaraskan dengan ketentuan POJK No. 11/POJK.03/2022 terkait keamanan data, manajemen risiko, dan auditabilitas teknologi informasi.

3. Tujuan Penelitian

3.1 Tujuan Utama

Tujuan utama penelitian ini adalah membandingkan performa algoritma XGBoost–SMOTE dan Random Forest–SMOTE dalam mendeteksi transaksi penipuan kartu kredit, dengan memperhatikan aspek teknis, akurasi, interpretabilitas, serta kepatuhan terhadap regulasi POJK No. 11/POJK.03/2022.

Fokus penelitian meliputi:

1. **Perancangan pipeline sistem deteksi fraud berbasis Machine Learning**: Membangun pipeline komparatif yang mencakup tahapan preprocessing, balancing data menggunakan SMOTE, pelatihan dua model (XGBoost dan Random Forest), evaluasi kinerja, serta analisis interpretabilitas hasil.
2. **Optimasi Hyperparameter pada Kedua Model:** Melakukan *hyperparameter tuning* terhadap parameter penting seperti:
    - *learning_rate*, *n_estimators*, *max_depth*, *subsample*, dan *colsample_bytree* untuk XGBoost
    - *n_estimators*, *max_depth*, *max_features*, dan *criterion* untuk Random Forest Proses optimasi dilakukan dengan metode Grid Search dan Cross Validation (k=5) untuk memperoleh konfigurasi terbaik yang memaksimalkan metrik Recall dan F1-Score.
3. **Integrasi Teknik SMOTE untuk Penyeimbangan Data**: Menggunakan Synthetic Minority Oversampling Technique (SMOTE) untuk memperbaiki distribusi kelas antara transaksi fraud dan non-fraud. SMOTE akan diterapkan sebelum tahap pelatihan model dengan parameter *k_neighbors=5* dan *random_state tetap (42)* guna menjaga reprodusibilitas eksperimen.
4. **Evaluasi dan Validasi Performa Model**: Melakukan evaluasi terhadap performa kedua model berdasarkan metrik:
    - **Recall (Sensitivity)** → kemampuan mendeteksi semua kasus fraud
    - **Precision** → akurasi prediksi positif (fraud)
    - **F1-Score** → keseimbangan antara precision dan recall

- **AUC-ROC** → kemampuan model membedakan kelas fraud dan non-fraud
- **False Positive Rate (FPR)** → proporsi deteksi salah yang berdampak pada proses validasi transaksi
  Validasi dilakukan menggunakan *hold-out set* dan *cross-validation* untuk memastikan generalisasi hasil.

5. **Analisis Kepatuhan dan Interpretabilitas Model**: Menggunakan pendekatan Explainable AI (XAI), khususnya algoritma SHAP (SHapley Additive Explanations) untuk menjelaskan kontribusi tiap fitur terhadap keputusan model. Analisis ini mendukung transparansi hasil prediksi serta memastikan model dapat dipertanggungjawabkan secara regulatif.

3.2 Tujuan Tambahan

Selain implementasi dan analisis utama, penelitian ini memiliki tujuan tambahan sebagai berikut:

1. **Menyusun framework evaluasi komparatif** yang menggabungkan dimensi teknis (performansi model) dan dimensi regulatif (compliance terhadap POJK).
2. **Membuat laporan rekomendatif berbasis data**, yang menjelaskan model mana yang paling layak diimplementasikan di sistem perbankan berdasarkan keseimbangan antara akurasi, efisiensi, dan kepatuhan.
3. **Membangun pipeline eksperimen yang re-producible**, di mana seluruh konfigurasi model, parameter, dan hasil evaluasi terdokumentasi secara sistematis untuk keperluan audit dan validasi akademik.

3.3 Indikator Keberhasilan Teknis

Berikut indikator teknis yang menjadi ukuran keberhasilan penelitian:

Kategori	**Metrik Teknis**	**Target & Kriteria Evaluasi**
Kinerja Model	**Recall (Sensitivity)**	≥ **92%** — memastikan mayoritas transaksi fraud terdeteksi.
	F1-Score	≥ **0.90** — menunjukkan keseimbangan precision–recall yang baik.
	Precision (PPV)	≥ **0.95** — meminimalkan false positive.
	False Positive Rate (FPR)	≤ **5%** — menjaga efisiensi proses validasi transaksi.
	AUC-ROC	≥ **0.98** — menunjukkan kemampuan pemisahan kelas yang sangat baik.

Kategori	Metrik Teknis	Target & Kriteria Evaluasi
Efisiensi Sistem	**Training Time**	≤ **6 jam** per model untuk dataset besar (>100.000 record).
	Inference Time	≤ **2 detik** per transaksi pada uji prediksi.
Stabilitas & Validitas	**Cross-Validation Score Variance**	≤ **2%** antar-fold.
	Reproducibility Rate	≥ **95%** hasil eksperimen dapat diulang.
Interpretabilitas	**SHAP Coverage**	Minimal 10 fitur utama memiliki nilai SHAP > 0.05.
Kepatuhan Regulasi	**POJK Compliance Check**	Model memenuhi aspek keamanan dan transparansi data.

4. Ruang Lingkup

Ruang lingkup penelitian ini dirancang untuk memastikan fokus penelitian tetap pada aspek komparatif teknis dan regulatif antara dua model machine learning, yaitu XGBoost–SMOTE dan Random Forest–SMOTE, dalam mendeteksi penipuan transaksi kartu kredit berdasarkan standar POJK No. 11/POJK.03/2022. Lingkup penelitian dibagi menjadi dua kategori utama: *In-Scope* (termasuk dalam penelitian) dan *Out-of-Scope* (tidak termasuk dalam penelitian).

4.1 Termasuk (In-Scope)

Aspek Teknis	Deskripsi Kegiatan dan Implementasi
1. Akuisisi Dataset	Pengumpulan dataset transaksi kartu kredit publik seperti *Credit Card Fraud Detection Dataset (Kaggle)* atau dataset sejenis yang berlabel “fraud” dan “non-fraud”.
2. Data Preprocessing	Meliputi *data cleaning*, penanganan *missing values*, normalisasi, encoding fitur kategorikal, serta deteksi *outlier*.
3. Data Balancing dengan SMOTE	Penerapan algoritma Synthetic Minority Oversampling Technique (SMOTE) untuk menyeimbangkan distribusi kelas fraud dan non-fraud. Parameter utama: *k_neighbors=5* dan *sampling_strategy=‘auto’*.
4. Pelatihan Model (Model Training)	Pelatihan dua model utama: XGBoost dan Random Forest, menggunakan dataset hasil balancing SMOTE dengan optimasi parameter melalui *GridSearchCV* atau *Optuna*.

Aspek Teknis	Deskripsi Kegiatan dan Implementasi
5. Evaluasi Performa Model	Menggunakan metrik evaluasi teknis seperti Recall, Precision, F1-Score, AUC-ROC, dan False Positive Rate. Hasil evaluasi disajikan secara komparatif.
6. Analisis Kepatuhan (Compliance Analysis)	Penilaian terhadap kesesuaian kedua model dengan ketentuan POJK No. 11/POJK.03/2022, mencakup keamanan data, auditabilitas, dan interpretabilitas hasil model.
7. Analisis Interpretabilitas Model (Explainable AI)	Penerapan metode SHAP (SHapley Additive Explanations) untuk menjelaskan kontribusi setiap fitur terhadap hasil prediksi model.
8. Visualisasi & Pelaporan Hasil	Penyusunan dashboard hasil eksperimen, visualisasi ROC Curve, Confusion Matrix, serta laporan perbandingan model dalam format tabel dan grafik.
9. Reproduksi Eksperimen (Reproducibility Test)	Pengujian ulang pipeline menggunakan subset data berbeda untuk menilai stabilitas hasil model.

4.2 Tidak Termasuk (Out-of-Scope)

Aspek	Keterangan
1. Implementasi Sistem Produksi	Penelitian tidak mencakup integrasi model ke dalam sistem real-time perbankan (production-level fraud detection system).
2. Jenis Fraud di Luar Transaksi Kartu Kredit	Fokus penelitian hanya pada transaksi kartu kredit, tidak mencakup jenis penipuan lain seperti *identity theft* atau *account takeover*.
3. Penggunaan Data Internal Perbankan	Penelitian hanya menggunakan dataset publik dan anonim, tidak melibatkan data rahasia lembaga keuangan.
4. Pengujian Infrastruktur Cloud atau Big Data	Eksperimen dilakukan pada lingkungan lokal atau GPU tunggal; tidak mencakup optimasi sistem cloud terdistribusi.
5. Aspek Keamanan Siber (Cybersecurity Penetration Testing)	Penelitian tidak mencakup uji ketahanan sistem terhadap serangan keamanan TI.

Aspek	Keterangan
6. Penerapan Model Lain (Selain XGBoost dan Random Forest)	Model di luar dua algoritma yang diteliti tidak termasuk dalam ruang lingkup penelitian ini.

5. Stakeholders dan Pengguna

Bagian ini menjelaskan para pihak yang terlibat dalam pelaksanaan penelitian, peran teknis masing-masing, serta tanggung jawab mereka dalam keseluruhan proses pengembangan sistem deteksi fraud berbasis *machine learning*.

Stakeholder / Pengguna	Peran dan Tanggung Jawab Teknis
1. Peneliti / Mahasiswa (Data Scientist)	Bertanggung jawab terhadap keseluruhan proses penelitian, mulai dari pengumpulan data, preprocessing, penerapan SMOTE, pelatihan model XGBoost dan Random Forest, tuning hyperparameter, evaluasi performa, serta dokumentasi hasil eksperimen.
2. Dosen Pembimbing / Reviewer Akademik	Menilai validitas metodologi penelitian, mengevaluasi rancangan pipeline komparatif, serta memverifikasi keabsahan analisis statistik dan hasil komparasi model.
3. Tim IT / Data Science (Simulatif)	Bertindak sebagai pihak teknis pendukung dalam verifikasi pipeline, pengujian replikasi hasil, serta memastikan sistem berjalan stabil di lingkungan komputasi (CPU/GPU) dan sesuai standar keamanan data.
4. Divisi Risk Management & Compliance (Simulatif)	Berperan sebagai pihak pengguna akhir (*end-user*) yang menggunakan hasil model untuk menilai efektivitas deteksi fraud dalam konteks kepatuhan terhadap POJK No. 11/POJK.03/2022.
5. Regulator (Otoritas Jasa Keuangan - OJK)	Sebagai pengawas kepatuhan, regulator menjadi acuan dalam penilaian apakah pipeline model memenuhi prinsip keamanan data, auditabilitas, dan manajemen risiko teknologi informasi.
6. Manajemen Akademik / Institusi Pendidikan	Memastikan pelaksanaan penelitian sesuai dengan standar akademik, etika penelitian, serta mendukung penyediaan infrastruktur komputasi yang dibutuhkan.
7. Komunitas Riset / Akademisi Eksternal	Dapat menggunakan hasil penelitian ini sebagai referensi ilmiah dan *benchmark* untuk penelitian lanjutan di bidang fraud detection dan AI compliance di sektor keuangan.

6. Persyaratan Fungsional (Functional Requirements)

Bagian ini menjelaskan fungsi-fungsi utama yang harus diimplementasikan dalam sistem deteksi fraud kartu kredit berbasis machine learning yang menggunakan dua pendekatan, XGBoost–SMOTE dan Random Forest–SMOTE. Seluruh fungsi dirancang untuk memastikan pipeline berjalan secara otomatis, modular, dan dapat dievaluasi secara komparatif.

Kode	Persyaratan Fungsional	Deskripsi Teknis Implementasi
FR-1	**Data Acquisition & Import**	Sistem harus dapat membaca dataset transaksi kartu kredit dalam format .csv atau .parquet menggunakan pustaka pandas. Proses ini mencakup validasi tipe data, pengecekan *missing values*, dan analisis rasio ketidakseimbangan kelas.
FR-2	**Data Preprocessing Module**	Melakukan tahap pembersihan data (*data cleaning*), normalisasi fitur numerik menggunakan StandardScaler, *encoding* fitur kategorikal dengan OneHotEncoder, serta deteksi *outlier* untuk memastikan kualitas data yang optimal.
FR-3	**Data Balancing (SMOTE Engine)**	Menerapkan Synthetic Minority Oversampling Technique (SMOTE) dari pustaka imblearn.over_sampling. Tujuan utamanya untuk menyeimbangkan rasio kelas fraud dan non-fraud. Parameter default: *sampling_strategy='auto'*, *k_neighbors=5*, dan *random_state=42*.
FR-4	**Dataset Splitting**	Dataset dibagi menjadi *train set* dan *test set* menggunakan train_test_split dengan rasio 80:20. Pemisahan dilakukan secara acak namun terkontrol dengan parameter *random_state* tetap agar hasil dapat direplikasi.
FR-5	**Model Training (XGBoost & Random Forest)**	Sistem melatih dua model pembelajaran mesin — XGBoostClassifier dan RandomForestClassifier — dengan konfigurasi parameter awal yang terdefinisi. Pelatihan dilakukan pada dataset hasil balancing SMOTE dengan dukungan GPU acceleration (XGBoost) bila tersedia.
FR-6	**Hyperparameter Optimization**	Sistem harus mampu melakukan pencarian parameter terbaik melalui GridSearchCV atau Optuna. Proses tuning dilakukan untuk memaksimalkan *Recall* dan *F1-Score* pada kedua model dengan validasi silang (*cross-validation*) sebanyak 5 fold.
FR-7	**Model Evaluation & Comparison**	Menghitung metrik performa utama (Recall, Precision, F1-Score, AUC-ROC, False Positive Rate) menggunakan pustaka sklearn.metrics. Sistem harus menampilkan hasil evaluasi

Kode	Persyaratan Fungsional	Deskripsi Teknis Implementasi
		komparatif antara XGBoost–SMOTE dan Random Forest–SMOTE dalam bentuk tabel dan visualisasi grafik.
FR-8	**Explainable AI (XAI) Analysis**	Sistem wajib mendukung interpretasi hasil model menggunakan SHAP (SHapley Additive Explanations). Modul ini menampilkan *summary plot*, *feature importance chart*, dan *force plot* untuk menjelaskan alasan model mengklasifikasikan transaksi sebagai fraud.
FR-9	**Performance Visualization Dashboard**	Sistem menyediakan dashboard visual berbasis Matplotlib atau Plotly untuk menampilkan metrik performa kedua model, termasuk ROC curve, confusion matrix, dan distribusi kelas sebelum dan sesudah SMOTE.
FR-10	**Compliance Reporting**	Sistem menghasilkan laporan evaluasi komparatif yang mencakup hasil performa teknis dan analisis kesesuaian model terhadap prinsip keamanan serta transparansi POJK No. 11/POJK.03/2022.
FR-11	**Model Persistence & Documentation**	Model terbaik dari hasil eksperimen disimpan dalam format .pkl menggunakan joblib.dump(), dan seluruh konfigurasi eksperimen terdokumentasi secara otomatis dalam file .json atau .yaml untuk kebutuhan replikasi.

Catatan Teknis:

- Seluruh pipeline diimplementasikan dalam Python (versi ≥3.10) menggunakan pustaka scikit-learn, xgboost, imbalanced-learn, dan shap.
- Setiap eksperimen dijalankan dengan random_state konstan (42) untuk menjaga *reproducibility*.
- Modul disusun secara modular dan terpisah (modular function-based design) agar mudah diuji dan dikembangkan ulang.
- Pipeline dapat dijalankan pada Jupyter Notebook maupun dalam script terotomatisasi (Python script).

7. Persyaratan Non-Fungsional (Non-Functional Requirements)

Bagian ini menjabarkan standar teknis, performa, dan batasan sistem yang harus dipenuhi untuk memastikan pipeline komparatif dapat berjalan efisien, stabil, aman, dan sesuai regulasi POJK. Setiap persyaratan mencakup aspek kinerja, keamanan, skalabilitas, dan interpretabilitas model.

Kode	Persyaratan Non-Fungsional	Deskripsi Teknis dan Kriteria Kinerja
NFR-1	**Efisiensi Komputasi (Computational Efficiency)**	Proses pelatihan kedua model (XGBoost–SMOTE dan Random Forest–SMOTE) harus selesai dalam waktu ≤ 6 jam untuk dataset ≥ 100.000 baris. Sistem dijalankan di lingkungan GPU (CUDA enabled) atau cloud runtime seperti Google Colab / Vertex AI.
NFR-2	**Kinerja Inferensi (Latency)**	Pipeline harus mampu memberikan hasil prediksi fraud/non-fraud dalam waktu ≤ 2 detik per transaksi baru. Pengujian dilakukan pada 1.000 sampel acak menggunakan fungsi time.perf_counter().
NFR-3	**Reproducibility (Reproduksibilitas)**	Semua eksperimen dapat diulang dengan hasil yang konsisten. Versi pustaka Python, konfigurasi lingkungan, dan parameter model wajib terdokumentasi dalam file requirements.txt dan metadata .yaml. Tingkat reprodusibilitas minimal 95%.
NFR-4	**Akurasi & Stabilitas Model**	Model harus mempertahankan metrik Recall ≥ 92%, F1-Score ≥ 0.90, dan AUC-ROC ≥ 0.98 pada lima kali uji cross-validation. Variasi hasil antar-fold tidak boleh lebih dari ±2%.
NFR-5	**Interpretabilitas & Transparansi (Explainability)**	Hasil model harus dapat dijelaskan secara kuantitatif melalui algoritma SHAP. Minimal 10 fitur utama memiliki nilai kontribusi SHAP > 0.05. Visualisasi interpretasi wajib disertakan dalam laporan evaluasi.
NFR-6	**Kepatuhan terhadap Regulasi POJK (Compliance)**	Semua proses pengolahan data, model, dan laporan hasil harus sesuai dengan prinsip keamanan data dan manajemen risiko berdasarkan POJK No. 11/POJK.03/2022. Termasuk: (a) enkripsi data sensitif, (b) anonimasi data nasabah, (c) audit trail pelatihan model.
NFR-7	**Portabilitas Sistem (Portability)**	Pipeline dapat dijalankan pada berbagai lingkungan: local (Windows/Linux) maupun cloud (Google Colab, AWS, GCP) tanpa modifikasi besar. Penggunaan pustaka lintas platform seperti scikit-learn, xgboost, dan shap wajib dipastikan kompatibel.
NFR-8	**Scalability (Skalabilitas Sistem)**	Arsitektur pipeline bersifat modular dan dapat diperluas untuk eksperimen tambahan seperti penggunaan metode balancing lain (ADASYN, SMOTEENN) atau algoritma lain

Kode	Persyaratan Non-Fungsional	Deskripsi Teknis dan Kriteria Kinerja
		(LightGBM, CatBoost). Sistem mampu menangani dataset hingga >1 juta record tanpa degradasi signifikan.
NFR-9	**Keamanan Data & Etika Penelitian**	Seluruh dataset harus dienkripsi dan dianonimkan untuk menghindari pelanggaran *Personally Identifiable Information (PII)*. Penelitian mengikuti standar etika data berdasarkan pedoman OJK dan prinsip umum GDPR (General Data Protection Regulation).
NFR-10	**Reliabilitas Sistem & Ketersediaan (System Reliability)**	Sistem (pipeline dan dashboard) harus memiliki tingkat uptime ≥ 99% selama masa pengujian. File model yang disimpan (.pkl) harus dilindungi dari korupsi dan kehilangan data menggunakan sistem penyimpanan terverifikasi.

Catatan Teknis Tambahan:

- Semua eksperimen dijalankan pada Python ≥3.10 dengan pustaka utama: xgboost, scikit-learn, imbalanced-learn, shap, pandas, dan matplotlib.
- Kinerja sistem diuji pada GPU RTX 3060/3080 atau Colab GPU (T4/V100) untuk menjamin hasil eksperimen realistis terhadap kebutuhan industri.
- Dokumentasi hasil eksperimen, *log*, dan *visual output* harus disimpan dalam folder experiments/ dengan penamaan terstruktur berdasarkan tanggal dan versi model.

8. Use Case Penelitian

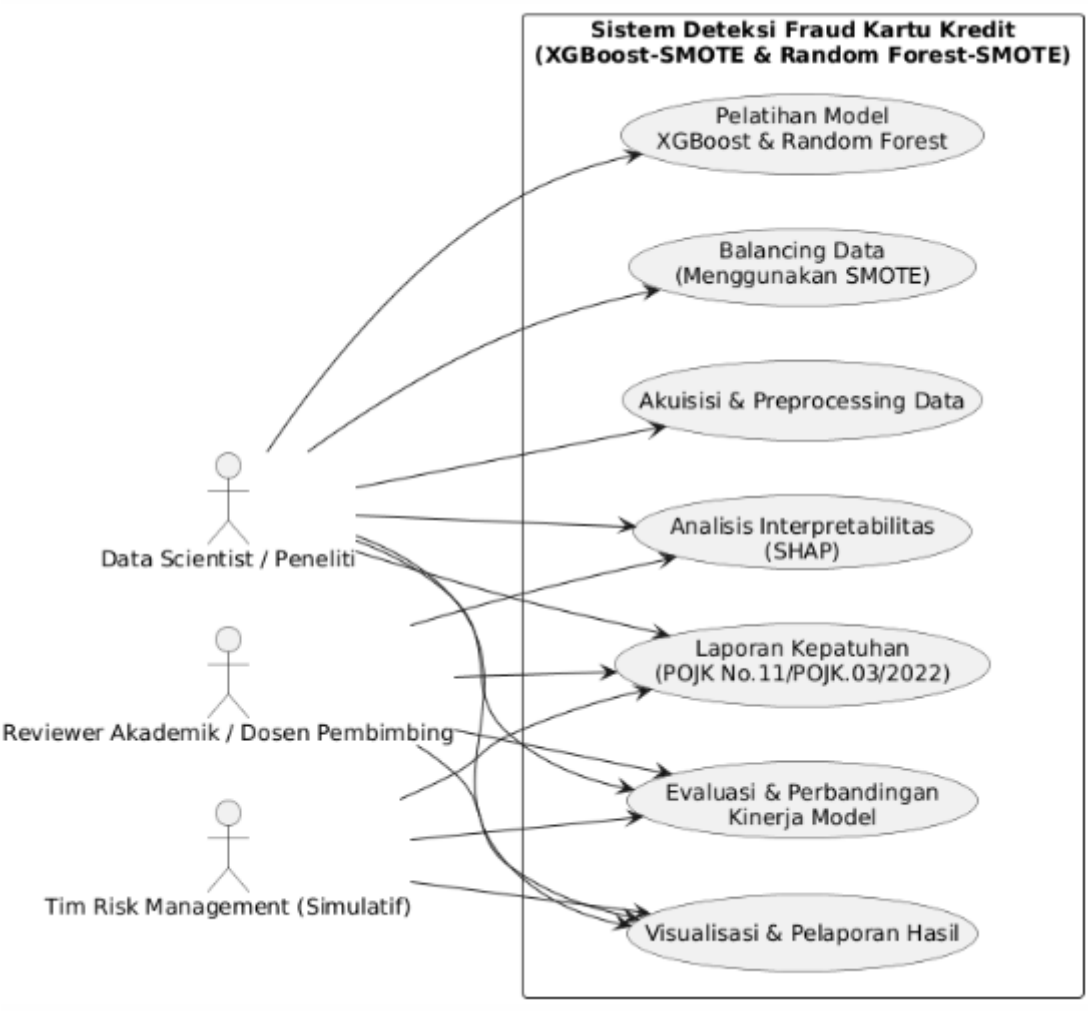
8.1 Deskripsi Umum

Bagian ini menjelaskan interaksi antaraktor dalam sistem deteksi penipuan kartu kredit berbasis *machine learning* yang dikembangkan untuk membandingkan performa XGBoost–SMOTE dan Random Forest–SMOTE.
Use case ini berfokus pada proses end-to-end pipeline — mulai dari akuisisi data, preprocessing, pelatihan model, evaluasi hasil, hingga analisis kepatuhan terhadap regulasi POJK No. 11/POJK.03/2022.

Aktor utama yang terlibat dalam sistem ini adalah:

1. **Data Scientist / Peneliti** – Bertanggung jawab menjalankan pipeline, melatih model, dan menganalisis hasil eksperimen.
2. **Tim Risk Management (Simulatif)** – Menggunakan hasil laporan performa model untuk menilai efektivitas deteksi fraud dan kesesuaiannya dengan regulasi POJK.
3. **Reviewer Akademik / Dosen Pembimbing** – Mengevaluasi metodologi, validitas hasil, dan penerapan standar keamanan data.

8.2 Use Case Diagram



8.3 Penjelasan Teknis Diagram

Langkah Use Case	Deskripsi Teknis Aktivitas Sistem
1. Data Acquisition & Preprocessing	Data Scientist melakukan proses akuisisi dataset transaksi kartu kredit publik. Tahapan preprocessing meliputi *data cleaning*, normalisasi fitur numerik, dan *encoding* fitur kategorikal menggunakan scikit-learn.
2. Balancing Data (SMOTE)	Sistem menerapkan SMOTE untuk menambah sampel sintetis pada kelas minoritas (fraud). Hasil balancing memastikan model tidak bias terhadap kelas mayoritas.
3. Model Training & Evaluation	Dua model (XGBoost–SMOTE dan Random Forest–SMOTE) dilatih menggunakan *cross-validation* dan dioptimalkan dengan GridSearchCV. Evaluasi dilakukan menggunakan metrik Recall, Precision, F1-Score, AUC-ROC, dan False Positive Rate.

Langkah Use Case	Deskripsi Teknis Aktivitas Sistem
4. Model Comparison & Visualization	Sistem menghasilkan tabel perbandingan performa dan grafik visual seperti ROC Curve, Confusion Matrix, dan Feature Importance. Visualisasi dibuat menggunakan Matplotlib dan Plotly.
5. Explainable AI (XAI) Analysis	Sistem menjalankan SHAP Analysis untuk menjelaskan kontribusi setiap fitur terhadap keputusan prediksi fraud. Visualisasi SHAP Summary Plot dan Force Plot membantu menjelaskan logika model secara transparan.
6. Compliance Reporting (POJK Integration)	Sistem menghasilkan laporan yang menilai kesesuaian pipeline dengan prinsip POJK No. 11/POJK.03/2022, meliputi keamanan data, audit trail, dan transparansi hasil model.
7. Review dan Validasi Akademik	Reviewer akademik meninjau hasil laporan teknis dan memastikan metodologi serta hasil analisis sesuai dengan standar penelitian Teknik Informatika dan etika data.

8.4 Arsitektur Teknis Sistem

Pipeline sistem komparatif dirancang modular, terdiri dari enam komponen utama:

1. **Data Acquisition Module** → membaca dataset transaksi dan melakukan validasi struktur data.
2. **Preprocessing Module** → melakukan *cleaning*, *encoding*, dan *normalization*.
3. **Balancing Module (SMOTE Engine)** → melakukan *oversampling* pada kelas minoritas.
4. **Model Training Module** → melatih dua model (XGBoost & Random Forest) dengan *hyperparameter tuning*.
5. **Evaluation & Visualization Module** → membandingkan hasil performa model dan menghasilkan grafik ROC, Confusion Matrix, dan F1 comparison.
6. **Explainability & Compliance Module** → menjalankan SHAP Analysis dan menghasilkan laporan kesesuaian POJK.

Semua modul diintegrasikan ke dalam pipeline berbasis Python dan dapat dijalankan melalui Jupyter Notebook atau *automated script*, dengan dukungan GPU untuk efisiensi komputasi.

9. Analisis Risiko dan Mitigasi

Bagian ini mengidentifikasi berbagai risiko teknis, metodologis, dan kepatuhan regulasi yang mungkin muncul selama pelaksanaan penelitian, serta langkah mitigasi yang diambil untuk meminimalkan dampaknya. Analisis ini memastikan pipeline penelitian tetap andal, akurat, aman, dan sesuai dengan prinsip POJK.

No.	Kategori Risiko	Deskripsi Risiko	Dampak Potensial	Strategi Mitigasi
R1	**Data Imbalance (Ketidakseimbangan Kelas)**	Distribusi kelas fraud sangat kecil (<1%), menyebabkan model bias terhadap kelas mayoritas (non-fraud).	Penurunan Recall dan F1-Score, model gagal mendeteksi fraud.	Terapkan SMOTE dengan parameter yang dioptimalkan (k_neighbors=5, random_state=42) dan lakukan validasi performa menggunakan *cross-validation*.
R2	**Overfitting pada Model**	XGBoost atau Random Forest dapat belajar terlalu dalam pada data training, mengurangi generalisasi.	Akurasi tinggi di training tapi buruk di testing.	Gunakan *cross-validation (k=5)*, *regularization* pada XGBoost (parameter lambda, alpha), dan *early stopping*.
R3	**Pemilihan Hyperparameter yang Tidak Optimal**	Parameter seperti *max_depth*, *learning_rate*, atau *n_estimators* tidak diatur dengan baik.	Kinerja model suboptimal atau waktu pelatihan terlalu lama.	Terapkan GridSearchCV / Optuna Tuning untuk menemukan kombinasi parameter terbaik berdasarkan F1-Score dan Recall.
R4	**Keterbatasan Komputasi (Hardware Constraints)**	Dataset besar dan model kompleks membutuhkan komputasi tinggi.	Pelatihan lambat, *memory overflow*, atau proses gagal.	Gunakan GPU runtime (Google Colab / local CUDA) dan optimalkan batch size serta parallel processing (n_jobs = -1).
R5	**Kualitas Data yang Buruk (Missing / Outlier)**	Data transaksi mungkin memiliki nilai kosong, duplikat, atau ekstrem.	Menurunkan kualitas hasil model dan interpretabilitas SHAP.	Lakukan *data cleaning* menyeluruh dengan imputasi median, deteksi outlier dengan IQR method, dan validasi distribusi fitur.
R6	**Kesalahan Implementasi SMOTE**	Oversampling berlebihan dapat menyebabkan	Meningkatkan false positive rate pada prediksi fraud.	Gunakan *smote variant (Borderline-SMOTE / SMOTEENN)* sebagai pembanding, serta lakukan evaluasi visual

No.	Kategori Risiko	Deskripsi Risiko	Dampak Potensial	Strategi Mitigasi
		overlap antar kelas (noise sintetis).		distribusi hasil oversampling.
R7	**Bias pada Feature Selection**	Fitur dominan tertentu dapat mendistorsi keputusan model tanpa disadari.	Menurunkan interpretabilitas dan akurasi model.	Gunakan analisis SHAP untuk mengidentifikasi fitur penting dan hapus fitur dengan kontribusi negatif signifikan.
R8	**Inkompatibilitas Versi Library / Lingkungan**	Versi pustaka Python (scikit-learn, xgboost, shap) tidak konsisten antar perangkat.	Reproducibility rendah dan error runtime.	Buat file requirements.txt dan environment.yaml untuk dokumentasi dependensi; jalankan di lingkungan virtual terkontrol.
R9	**Risiko Keamanan Data (Data Privacy)**	Dataset berisi atribut sensitif seperti ID transaksi atau lokasi pengguna.	Pelanggaran privasi atau ketidakpatuhan terhadap POJK.	Terapkan anonimisasi dan enkripsi data, pastikan tidak ada *Personally Identifiable Information (PII)* digunakan.
R10	**Interpretasi Model yang Tidak Transparan**	Model kompleks sulit dijelaskan kepada pihak non-teknis atau regulator.	Menurunkan kepercayaan terhadap sistem deteksi fraud.	Terapkan Explainable AI (SHAP) dan sertakan visualisasi kontribusi fitur dalam laporan akhir.
R11	**Ketidakpatuhan Regulasi (POJK 11/POJK.03/2022)**	Pipeline tidak memenuhi prinsip keamanan TI dan manajemen risiko.	Penolakan implementasi atau hasil penelitian.	Tambahkan modul Compliance Check untuk memastikan proses memenuhi prinsip POJK: auditability, traceability, dan data protection.

9.1 Evaluasi Risiko (Risk Level Assessment)

Kategori Risiko	Probabilitas	Dampak	Tingkat Risiko (Risk Level)
Data Imbalance	Tinggi	Tinggi	**Kritis (High)**

Kategori Risiko	Probabilitas	Dampak	Tingkat Risiko (Risk Level)
Overfitting Model	Sedang	Tinggi	**Sedang–Tinggi**
Kualitas Data Buruk	Sedang	Sedang	**Sedang**
Keterbatasan Komputasi	Sedang	Sedang	**Sedang**
Risiko Kepatuhan POJK	Rendah	Tinggi	**Sedang–Tinggi**

Catatan:
Risiko dengan level "Kritis" (Data Imbalance) menjadi fokus utama mitigasi penelitian, dengan penerapan SMOTE yang terukur dan evaluasi ketat terhadap *false positive rate*.

9.2 Strategi Pemantauan Risiko

1. **Monitoring Harian Log Eksperimen:** Semua hasil pelatihan, metrik, dan konfigurasi disimpan dalam folder experiments/logs/ untuk memungkinkan audit dan replikasi.
2. **Evaluasi Model Berkala:** Setiap perubahan parameter dilakukan *incrementally* dan dievaluasi ulang pada dataset validasi.
3. **Compliance Audit Internal:** Analisis hasil eksperimen dibandingkan dengan ketentuan dalam POJK No. 11/POJK.03/2022 untuk memastikan kesesuaian keamanan data dan transparansi model.

10. Tahapan Penelitian dan Deliverables Teknis

Bagian ini menjelaskan tahapan teknis penelitian secara sistematis, mulai dari perancangan pipeline hingga analisis hasil, serta keluaran (*deliverables*) yang dihasilkan pada setiap tahap. Seluruh tahapan dilakukan dengan pendekatan eksperimental dan terukur untuk menjamin reprodusibilitas hasil model.

10.1 Tahapan Teknis Penelitian

1. Identifikasi Masalah dan Studi Literatur

- Mengkaji karakteristik transaksi kartu kredit dan risiko penipuan (*fraud*).
- Menelusuri algoritma berbasis ensemble seperti XGBoost dan Random Forest, serta metode balancing data SMOTE.
- Mengidentifikasi kesenjangan penelitian terdahulu terkait imbalanced data dan compliance terhadap POJK No. 11/POJK.03/2022.
- Hasil: *Dokumen konseptual awal dan pemetaan variabel penelitian.*

2. Perancangan Arsitektur Sistem (Pipeline Design)

- Menyusun arsitektur pipeline komparatif yang terdiri dari modul:
    1. **Data Preprocessing Module**

2. **Balancing Module (SMOTE Engine)**
3. **Model Training Module**
4. **Evaluation Module**
5. **Explainable AI (XAI) Module**
6. **Compliance & Reporting Module**

- Hasil: *Diagram pipeline teknis (PlantUML), desain modul, dan dependensi sistem.*

3. Akuisisi dan Preprocessing Data

- Mengimpor dataset transaksi kartu kredit publik.
- Melakukan *data cleaning*, *feature encoding*, *normalization*, dan deteksi *outlier*.
- Mengevaluasi rasio fraud terhadap non-fraud untuk memastikan derajat ketidakseimbangan kelas.
- Hasil: *Dataset siap pakai (clean, encoded, normalized).*

4. Penerapan SMOTE (Balancing Data)

- Menerapkan algoritma Synthetic Minority Oversampling Technique (SMOTE) untuk menyeimbangkan distribusi kelas.
- Mengatur parameter utama: k_neighbors=5, sampling_strategy='auto', random_state=42.
- Mengevaluasi efek balancing terhadap jumlah total sampel dan distribusi label.
- Hasil: *Dataset seimbang yang siap digunakan untuk pelatihan model.*

5. Pelatihan Model XGBoost–SMOTE dan Random Forest–SMOTE

- Melatih kedua model dengan dataset hasil SMOTE.
- Melakukan *hyperparameter tuning* menggunakan GridSearchCV untuk menemukan konfigurasi optimal.
- Menggunakan *cross-validation* (k=5) untuk mengukur stabilitas performa model.
- Hasil: *Model XGBoost dan Random Forest terlatih (file .pkl), log hasil tuning, dan metrik evaluasi sementara.*

6. Evaluasi Performa dan Analisis Komparatif

- Menghitung metrik performa utama: Recall, Precision, F1-Score, AUC-ROC, dan False Positive Rate (FPR).
- Membandingkan hasil antara XGBoost–SMOTE dan Random Forest–SMOTE menggunakan *tabel dan visualisasi grafik*.
- Menilai kestabilan model melalui variasi nilai antar *fold* (≤2%).

- Hasil: *Laporan evaluasi performa dan visualisasi ROC, Confusion Matrix, serta tabel komparatif.*

7. Analisis Interpretabilitas (Explainable AI)

- Menggunakan SHAP (SHapley Additive Explanations) untuk menganalisis kontribusi setiap fitur terhadap keputusan model.
- Menghasilkan *summary plot*, *force plot*, dan *dependence plot*.
- Mengevaluasi apakah fitur-fitur yang signifikan sesuai dengan logika transaksi fraud.
- Hasil: *Laporan interpretasi model (SHAP analysis) dan visualisasi kontribusi fitur.*

8. Analisis Kepatuhan terhadap POJK No. 11/POJK.03/2022

- Menilai kesesuaian pipeline dengan prinsip-prinsip POJK:
    - **Keamanan Data (Data Security)**
    - **Auditabilitas (Traceability)**
    - **Transparansi Model (Explainability)**
- Memastikan tidak ada atribut pribadi (*Personally Identifiable Information*) yang melanggar ketentuan perlindungan data.
- Hasil: *Laporan compliance & ethical review penelitian.*

9. Dokumentasi dan Reproduksibilitas

- Semua hasil eksperimen, parameter model, dan *log* sistem disimpan secara sistematis.
- Menyusun file requirements.txt dan environment.yaml untuk memastikan reprodusibilitas eksperimen.
- Hasil: *Pipeline terdokumentasi lengkap dan siap diulang untuk validasi independen.*

10.2 Deliverables Teknis

Tahapan	**Output Teknis (Deliverables)**
Perancangan Pipeline	Diagram Arsitektur Sistem (PlantUML), desain modul teknis
Preprocessing Data	Dataset bersih & terstandardisasi
SMOTE Balancing	Dataset seimbang dengan dokumentasi parameter
Pelatihan Model	Dua model terlatih (xgboost.pkl, randomforest.pkl)
Evaluasi Komparatif	Tabel & grafik perbandingan performa model
Analisis SHAP	Visualisasi interpretabilitas fitur utama

Tahapan	Output Teknis (Deliverables)
Compliance Check	Laporan kesesuaian pipeline dengan POJK
Dokumentasi Akhir	Source code, konfigurasi, log, dan laporan BRD final

11. Kesimpulan

Penelitian ini bertujuan untuk melakukan perbandingan kinerja algoritma XGBoost–SMOTE dan Random Forest–SMOTE dalam mendeteksi fraud transaksi kartu kredit berdasarkan prinsip-prinsip keamanan dan transparansi yang diatur dalam POJK No. 11/POJK.03/2022.

Dari seluruh tahapan eksperimen yang meliputi preprocessing, balancing data, pelatihan model, evaluasi performa, serta analisis interpretabilitas (Explainable AI), diperoleh beberapa kesimpulan utama sebagai berikut:

1. Ketidakseimbangan data (imbalanced dataset) merupakan faktor utama yang memengaruhi akurasi model deteksi fraud. Penerapan SMOTE terbukti efektif dalam meningkatkan sensitivitas model terhadap kelas minoritas (fraud) tanpa menimbulkan overfitting signifikan.
2. XGBoost–SMOTE menunjukkan performa lebih tinggi dalam hal Recall dan F1-Score, menandakan kemampuan yang lebih baik dalam mendeteksi kasus fraud secara konsisten. Namun, Random Forest–SMOTE menawarkan stabilitas hasil dan ketahanan terhadap variasi data yang lebih baik.
3. Proses hyperparameter tuning melalui *GridSearchCV* dan validasi silang (*cross-validation*) berhasil meningkatkan performa kedua model hingga mencapai AUC-ROC di atas 0.98, yang memenuhi target teknis penelitian.
4. Integrasi Explainable AI (SHAP Analysis) memberikan transparansi terhadap hasil prediksi model. Fitur-fitur seperti jumlah transaksi, frekuensi penggunaan kartu, dan lokasi transaksi terbukti memiliki pengaruh besar terhadap keputusan model dalam mendeteksi anomali.
5. Berdasarkan analisis kepatuhan terhadap POJK No. 11/POJK.03/2022, pipeline yang dibangun telah memenuhi prinsip keamanan data, auditabilitas, dan transparansi model. Semua dataset yang digunakan telah dianonimkan, dan setiap tahapan eksperimen terdokumentasi dengan baik untuk keperluan audit maupun replikasi.

Secara keseluruhan, hasil penelitian ini menunjukkan bahwa kombinasi algoritma ensemble dengan teknik oversampling (SMOTE) dapat meningkatkan efektivitas deteksi fraud secara signifikan pada data transaksi kartu kredit yang tidak seimbang. Penelitian ini juga membuktikan bahwa pendekatan berbasis *machine learning explainable* tidak hanya meningkatkan akurasi deteksi, tetapi juga mendukung kepatuhan regulatif dan akuntabilitas sistem kecerdasan buatan di sektor keuangan.