

TINJAUAN SISTEMATIS: ANALISIS SWOT DAN KESENJANGAN UNTUK PERBANDINGAN ALGORITMA XGBOOST-SMOTE DAN RANDOM FOREST-SMOTE PADA DETEKSI FRAUD TRANSAKSI KARTU KREDIT BERDASARKAN STANDAR POJK NO. 11/POJK.03/2022

1. Pendahuluan

Tingginya volume transaksi kartu kredit digital telah meningkatkan risiko penipuan, menciptakan kebutuhan mendesak akan sistem deteksi yang akurat dan compliant dengan regulasi perbankan. POJK No. 11/POJK.03/2022 tentang Penerapan Teknologi Informasi oleh Bank Umum menetapkan standar keamanan TI yang harus dipatuhi perbankan Indonesia. Machine learning dengan teknik handling imbalance data seperti SMOTE menjadi solusi potensial, namun diperlukan analisis komparatif mendalam antara algoritma XGBoost dan Random Forest dalam konteks compliance regulasi ini.

2. Metodologi

Tujuh artikel penelitian terindeks dengan Digital Object Identifiers (DOI) dianalisis secara sistematis. Studi-studi ini mengeksplorasi penerapan machine learning, resampling techniques, dan aspek regulasi untuk deteksi penipuan kartu kredit. Sintesis temuan difokuskan pada analisis komparatif XGBoost-SMOTE vs Random Forest-SMOTE dan keselarasan dengan framework POJK No. 11/POJK.03/2022.

3. Sintesis Temuan

Tabel di bawah ini mensintesis temuan inti dari lima tinjauan yang menjadi dasar analisis ini.

| DOI / Sitasi | Temuan Inti | Penekanan Utama |
|--------------------------------------|--|--|
| 10.29207/resti.v6i6.4213 | Recall improved dari 81.63% (Random Forest) menjadi 92% (Gradient Boosting); SMOTE untuk optimasi data | Bukti empiris perbandingan performa Random Forest vs boosting techniques |
| 10.7717/peerj-cs.1278 | ML dan deep learning populer untuk deteksi fraud kartu kredit; review 181 artikel (2019-2021) | Konteks penelitian terkini dan identifikasi gap metodologi |
| 10.3390/fi16060196 | Federated learning + blockchain dengan Random Forest + SMOTE meningkatkan performa | Validasi efektivitas Random Forest-SMOTE dalam architecture modern |
| 10.3390/math10132272 | Hybrid ML + swarm metaheuristic (XGBoost + SMOTE) menunjukkan hasil superior | Bukti keunggulan XGBoost-SMOTE dengan optimasi parameter |
| 10.3390/technologies13030088 | XGBoost + SMOTE konsisten capai F1 score tertinggi di semua level imbalance | Pembandingan langsung XGBoost vs Random Forest dengan SMOTE |
| 10.35877/soshum2169 | Analisis hukum perlindungan data nasabah perbankan dan kerangka POJK | Dasar regulasi untuk evaluasi compliance sistem deteksi fraud |
| 10.1080/17521440.2020.1760454 | Kebutuhan pendekatan proaktif regulasi AI di sektor finansial | Konteks regulatory gap untuk implementasi AI-based fraud detection |

4. Analisis SWOT

| Dimensi | Analisis |
|-------------------------|---|
| Kekuatan (Strengths) | <ul style="list-style-type: none"> S1. Kinerja Teknis Terbukti: XGBoost-SMOTE mencapai F1 score tertinggi dan robust di berbagai tingkat ketidakseimbangan data S2. Peningkatan Signifikan: Boosting techniques meningkatkan recall hingga 92% dibanding Random Forest (81.63%) S3. Dukungan Regulasi: POJK No. 11/POJK.03/2022 memberikan landasan hukum implementasi sistem deteksi fraud S4. Optimasi Efektif: Teknik metaheuristic (Group Search Firefly) terbukti meningkatkan performa hybrid model |
| Kelemahan (Weaknesses) | <ul style="list-style-type: none"> W1. Keterbatasan Proteksi Data: Regulasi existing belum memberikan panduan teknis implementasi yang komprehensif W2. Variasi Performa: Random Forest menunjukkan recall lebih rendah dibanding algoritma boosting W3. Kompleksitas Implementasi: Integrasi sistem deteksi dengan framework regulasi yang kompleks W4. Sumber Daya Komputasi: Proses training dan tuning memerlukan computational resources signifikan |
| Peluang (Opportunities) | <ul style="list-style-type: none"> O1. Framework Evaluasi Baru: Mengembangkan framework evaluasi yang mengintegrasikan aspek teknis dan compliance POJK O2. Optimasi Lanjutan: Potensi tuning lebih lanjut dengan berbagai algoritma optimasi untuk kedua algoritma O3. Integrasi Teknologi Emerging: Kombinasi dengan federated learning dan blockchain untuk enhanced security O4. Standardisasi Benchmark: Menetapkan protokol standar evaluasi sesuai requirement POJK |
| Ancaman (Threats) | <ul style="list-style-type: none"> T1. Regulatory Gap: Kurangnya transisi prinsip AI governance ke implementasi praktis T2. Evolusi Teknik Fraud: Perkembangan metode penipuan membutuhkan continuous improvement sistem T3. Data Privacy Concerns: Risiko pencurian data selama proses transaksi dan training model |

| | |
|--|---|
| | <ul style="list-style-type: none"> T4. Kompleksitas Compliance: Tantangan memenuhi seluruh requirement POJK dalam sistem ML |
|--|---|

5. Analisis Kesenjangan (Gap Analysis)

Analisis ini mengidentifikasi kesenjangan kritis dalam lanskap penelitian saat ini yang perlu diatasi agar bidang ini dapat matang.

| Kategori Kesenjangan | Kesenjangan yang Teridentifikasi | Bukti dari Data yang Disediakan |
|--|---|---|
| Kesenjangan Evaluasi Komparatif | Tidak ada studi yang secara spesifik membandingkan XGBoost-SMOTE vs Random Forest-SMOTE dalam konteks compliance POJK | Beberapa studi (10.3390/technologies13030088) membandingkan beberapa teknik, namun tidak secara khusus mendalam membandingkan semua dalam konteks hybrid dengan XGBoost untuk kartu kredit. |
| Kesenjangan Framework Regulasi-Teknis | Belum ada framework evaluasi yang menghubungkan performance metrics dengan requirements POJK No. 11/POJK.03/2022 | Meski dinyatakan robust (10.3390/technologies13030088), tidak ada analisis mendalam tentang batasan robustness-nya terhadap drift konsep atau imbalance yang sangat ekstrem. |
| Kesenjangan Validasi Compliance | Tidak ada protokol validasi yang menghubungkan efektivitas algoritma dengan standar perlindungan data nasabah | Tidak satu pun penelitian yang disintesis membahas metode <i>Explainable AI</i> (XAI) untuk menjelaskan prediksi dari model XGBoost-SMOTE. |
| Kesenjangan Implementasi Industri | Kesenjangan antara hasil akademis dengan panduan implementasi praktis di industri perbankan | Kompleksitas komputasional disebut sebagai kelemahan (W1), tetapi tidak ada solusi efisiensi yang diusulkan secara mendalam dalam literatur yang ditinjau. |
| Kesenjangan Robustness Ekstrem | Tidak ada analisis mendalam tentang performa algoritma pada tingkat ketidakseimbangan sangat ekstrem | Semua penelitian berfokus pada kinerja algoritmik, bukan pada jalur implementasi, <i>model deployment</i> , atau integrasi dengan sistem produksi. |

6. Kesimpulan

Bidang deteksi fraud kartu kredit menunjukkan kekuatan teknis yang menjanjikan dengan XGBoost-SMOTE, namun menghadapi tantangan implementasi dalam kerangka regulasi POJK No. 11/POJK.03/2022. Kesenjangan kritis teridentifikasi dalam evaluasi komparatif spesifik antara XGBoost-SMOTE dan Random Forest-SMOTE, serta integrasi aspek teknis dengan requirements regulasi. Penelitian ini diharapkan dapat mengisi kesenjangan tersebut dengan memberikan analisis komparatif komprehensif yang selaras dengan standar POJK, sekaligus memberikan rekomendasi implementasi bagi industri perbankan Indonesia.