KAMPUS AKADEMIK PUBLISING
Jurnal Ilmiah Nusantara (JINU)
Vol.2, No.3 Mei 2025
e-ISSN: 3047-7603, p-ISSN :3047-9673, Hal 35-49
DOI : https://doi.org/10.61722/jinu.v2i3.4276

ANALISIS KINERJA MODEL MACHINE LEARNING UNTUK MENDETEKSI TRANSAKSI FRAUD PADA SISTEM PEMBAYARAN ONLINE

Maulana Malik Ibrahim
043493218@ecampus.ut.ac.id
Universitas Terbuka
Sony Alfauzan
043491633@ecampus.ut.ac.id
Universitas Terbuka

Abstract *The rapid growth of digital transactions has led to an increase in fraudulent activities within online payment systems. Traditional fraud detection methods based on rule-based systems have limitations in identifying evolving fraud patterns. This study aims to analyze the performance of various Machine Learning (ML) models in detecting fraudulent transactions using the Online Payment Fraud Detection Dataset from Kaggle. The models tested include Logistic Regression, Decision Tree, Random Forest, XGBoost, Support Vector Machine (SVM), and Bidirectional Long Short-Term Memory (BiLSTM). The study also evaluates the impact of data balancing techniques, namely Synthetic Minority Oversampling Technique (SMOTE) and Random Undersampling, on model performance. The results indicate that XGBoost and BiLSTM achieved the highest F1-scores of 88% and 90%, respectively, with SMOTE significantly improving recall rates. These findings suggest that ML can be effectively applied to financial security systems, with XGBoost being more suitable for real-time fraud detection, while BiLSTM excels in identifying complex transaction patterns. Future research should focus on optimizing computational efficiency and exploring Explainable AI techniques to enhance model interpretability.*
Keywords: *Data Balancing, Fraud Detection, Machine Learning, Online Payment, XGBoost*

Abstrak Pesatnya pertumbuhan transaksi digital telah meningkatkan aktivitas fraud dalam sistem pembayaran online. Metode deteksi fraud berbasis aturan memiliki keterbatasan dalam mengenali pola kejahatan yang terus berkembang. Penelitian ini bertujuan untuk menganalisis kinerja berbagai model Machine Learning dalam mendeteksi transaksi fraud menggunakan dataset Online Payment Fraud Detection dari Kaggle. Model yang diuji meliputi Logistic Regression, Decision Tree, Random Forest, XGBoost, Support Vector Machine (SVM), dan Bidirectional Long Short-Term Memory (BiLSTM). Studi ini juga mengevaluasi pengaruh teknik balancing data, yaitu Synthetic Minority Oversampling Technique (SMOTE) dan Random Undersampling, terhadap performa model. Hasil penelitian menunjukkan bahwa XGBoost dan BiLSTM mencapai F1-score tertinggi, masing-masing sebesar 88% dan 90%, dengan SMOTE yang secara signifikan meningkatkan recall. Temuan ini mengindikasikan bahwa Machine Learning dapat diterapkan secara efektif dalam sistem keamanan keuangan, di mana XGBoost lebih cocok untuk deteksi fraud secara real-time, sedangkan BiLSTM unggul dalam mengidentifikasi pola transaksi yang lebih kompleks. Penelitian selanjutnya disarankan untuk mengoptimalkan efisiensi komputasi serta mengeksplorasi Explainable AI guna meningkatkan interpretabilitas model.
Kata kunci: *Balancing Data, Deteksi Fraud, Machine Learning, Pembayaran Online, XGBoost*

LATAR BELAKANG

Pertumbuhan teknologi digital telah mengubah lanskap transaksi keuangan, terutama melalui sistem pembayaran online. Menurut Statista (2023), nilai transaksi digital global diperkirakan akan melampaui $10 triliun pada tahun 2025, didorong oleh adopsi e-commerce, dompet digital, dan sistem pembayaran elektronik. Namun, peningkatan transaksi ini diiringi dengan lonjakan kasus penipuan, seperti carding,

Received Maret 28, 2024; Revised April 12, 2024; Mei 01, 2025
* Maulana Malik Ibrahim, 043493218@ecampus.ut.ac.id

phishing, dan identity theft, yang semakin kompleks dan sulit diantisipasi oleh sistem deteksi konvensional.

Sistem deteksi fraud tradisional yang mengandalkan aturan baku (rule-based systems) memiliki keterbatasan dalam mengenali pola penipuan baru, sehingga menciptakan gap antara kebutuhan keamanan saat ini dan kemampuan teknologi yang ada. Penelitian-penelitian terbaru telah mengadopsi pendekatan Machine Learning untuk mengatasi permasalahan tersebut, namun masih banyak studi yang hanya fokus pada evaluasi kinerja model tanpa mengeksplorasi secara mendalam pengaruh teknik balancing data terhadap performa deteksi.

Kebaruan penelitian ini terletak pada analisis komprehensif pengaruh teknik balancing data—seperti SMOTE dan Random Undersampling—terhadap akurasi dan recall model deteksi fraud, serta perbandingan antara model ensemble (misalnya XGBoost) dan pendekatan deep learning (seperti BiLSTM) dalam konteks transaksi online. Dengan mengisi gap tersebut, penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam pengembangan sistem keamanan yang lebih adaptif dan efektif untuk mendeteksi transaksi fraud di era digital.

KAJIAN TEORITIS

2.1 Konsep Dasar Deteksi Fraud dalam Transaksi Online

Fraud dalam transaksi online merupakan bentuk kejahatan keuangan yang dilakukan dengan cara memanipulasi informasi transaksi untuk mendapatkan keuntungan secara ilegal (*Janardhanan, 2025*). Fraud dapat terjadi dalam berbagai bentuk, seperti:

a. Carding: Penggunaan ilegal data kartu kredit untuk melakukan transaksi tanpa izin pemilik kartu.
b. Phishing: Penipuan yang melibatkan pencurian kredensial pengguna melalui situs web palsu atau email.
c. Identity Theft: Penggunaan identitas orang lain untuk melakukan transaksi keuangan.

Menurut Reyhan & Ahmad (2024), sistem konvensional dalam mendeteksi fraud masih banyak yang mengandalkan pendekatan rule-based, yang bekerja dengan mengidentifikasi pola transaksi mencurigakan berdasarkan aturan yang telah ditentukan sebelumnya. Namun, metode ini memiliki beberapa kelemahan, antara lain:

a. Sulit beradaptasi dengan pola penipuan baru.
b. Tingkat false positive tinggi (transaksi sah diklasifikasikan sebagai fraud).
c. Membutuhkan pemeliharaan aturan secara manual, yang tidak efisien untuk skala besar.

Oleh karena itu, pendekatan berbasis Machine Learning menjadi solusi yang lebih efektif karena mampu mengidentifikasi pola transaksi secara otomatis, bahkan untuk skenario yang belum pernah terjadi sebelumnya (*Putra, 2024*).

2.2 Machine Learning dalam Deteksi Fraud

Machine Learning (ML) adalah cabang kecerdasan buatan yang memungkinkan komputer untuk belajar dari data dan membuat keputusan tanpa pemrograman eksplisit (*Afridah, 2024*). Dalam konteks deteksi fraud, ML digunakan untuk mengidentifikasi pola transaksi mencurigakan dan mengklasifikasikan transaksi sebagai fraud atau non-fraud.

Menurut Ghosh Dastidar (2025), pendekatan Machine Learning dalam deteksi fraud dapat dikategorikan sebagai berikut:

a. Supervised Learning: Model dilatih menggunakan data historis yang sudah dilabeli (fraud/non-fraud).
b. Unsupervised Learning: Model mencari pola anomali tanpa label eksplisit.
c. Semi-Supervised Learning: Kombinasi dari supervised dan unsupervised learning untuk meningkatkan akurasi model.

Pada penelitian ini, digunakan pendekatan Supervised Learning, karena dataset yang digunakan telah memiliki label fraud dan non-fraud.

2.3 Model Machine Learning yang Digunakan dalam Penelitian Ini

Berbagai model Machine Learning telah dikembangkan untuk mendeteksi fraud dalam transaksi online. Beberapa model utama yang digunakan dalam penelitian ini adalah:

Model	Kategori	Keunggulan	Kelemahan
Logistic Regression	Model linear	Mudah diinterpretasikan, cepat	Kurang efektif untuk data non-linear
Decision Tree	Pohon Keputusan	Mudah dipahami, cocok untuk data kompleks	Rentan terhadap overfitting

Model	Kategori	Keunggulan	Kelemahan
Random Forest	Ensemble Learning (Bagging)	Lebih stabil, menangani fitur non-linear dengan baik	Waktu komputasi lebih lama
XGBoost	Boosting Algorithm	Sangat kuat untuk deteksi fraud, menangani class imbalance	Memerlukan tuning parameter yang lebih kompleks
SVM (Support Vector Machine)	Kernel-based Model	Efektif untuk dataset dengan dimensi tinggi	Tidak efisien untuk dataset besar
BiLSTM (Bidirectional LSTM)	Deep Learning	Mampu menangkap pola transaksi yang kompleks	Membutuhkan daya komputasi tinggi

Menurut Polu (2025), metode Random Forest dan XGBoost merupakan salah satu algoritma terbaik dalam deteksi fraud, karena mampu menangani data yang tidak seimbang dan fitur dengan hubungan non-linear. Selain itu, BiLSTM memiliki keunggulan dalam mengenali pola transaksi dalam bentuk sekuensial, sehingga lebih baik dalam mendeteksi fraud yang melibatkan perubahan perilaku pengguna.

2.4 Tantangan dalam Penerapan Machine Learning untuk Deteksi Fraud

Ketidakseimbangan Data (Class Imbalance)

a. Salah satu tantangan utama dalam deteksi fraud adalah ketidakseimbangan data, di mana jumlah transaksi fraud jauh lebih sedikit dibandingkan transaksi normal (*Kurniawan, 2024*).
b. Jika tidak ditangani dengan baik, model akan lebih cenderung mengabaikan transaksi fraud, yang menyebabkan tingkat recall rendah.
c. Solusi yang digunakan dalam penelitian ini adalah SMOTE (Synthetic Minority Oversampling Technique) dan Random Undersampling, yang bertujuan untuk menyeimbangkan distribusi kelas.

Overfitting pada Model Machine Learning

a. Beberapa algoritma seperti Decision Tree dan Neural Networks memiliki kecenderungan untuk mempelajari detail terlalu dalam dari data pelatihan, sehingga performanya menurun pada data baru.

b. Untuk mengatasi ini, dilakukan hyperparameter tuning serta diterapkan Stratified K-Fold Cross Validation guna meningkatkan generalisasi model (*Billah, 2024*).

Kurangnya Interpretabilitas Model AI

a. Salah satu kelemahan model Machine Learning berbasis Deep Learning seperti Neural Networks adalah kurangnya interpretabilitas dalam pengambilan keputusan.
b. Untuk mengatasi masalah ini, penelitian ini merekomendasikan Explainable AI (SHAP, LIME) untuk memahami faktor-faktor yang memengaruhi prediksi model.

2.5 Penelitian Sebelumnya yang Relevan

Beberapa penelitian sebelumnya yang menjadi referensi utama dalam penelitian ini adalah:

Penelitian	Metode yang Digunakan	Hasil Utama
Afridah (2024)	CART dan Naïve Bayes dengan PSO	Optimasi dengan Particle Swarm Optimization meningkatkan akurasi deteksi fraud
Putra (2024)	Random Forest dan XGBoost	Model berbasis ensemble learning memiliki performa lebih baik dibanding model linear
Ghosh Dastidar (2025)	Model berbasis konteks dalam deteksi fraud	Menggunakan variabel tambahan seperti perilaku pengguna meningkatkan akurasi model
Janardhanan (2025)	Deep Learning untuk deteksi fraud	Model BiLSTM lebih unggul dalam menangani data transaksi berbasis waktu
Reyhan & Ahmad (2024)	Analisis big data dalam strategi keuangan	Big data membantu dalam meningkatkan akurasi prediksi fraud

Kesimpulan dari penelitian sebelumnya:

a. Model berbasis ensemble learning (Random Forest, XGBoost) memberikan hasil lebih akurat dalam deteksi fraud.

b. Deep Learning (BiLSTM) memiliki potensi besar dalam menangani pola transaksi yang lebih kompleks.
c. Teknik balancing data sangat penting untuk meningkatkan recall model.

2.6 Implikasi Kajian Teoritis terhadap Penelitian Ini

Hipotesis Tidak Tersurat:

a. Model Machine Learning yang lebih kompleks, seperti XGBoost dan BiLSTM, akan memiliki performa lebih tinggi dibandingkan model yang lebih sederhana seperti Logistic Regression dan Decision Tree.
b. Teknik balancing data (SMOTE dan Random Undersampling) akan meningkatkan recall dalam mendeteksi transaksi fraud.
c. Interpretabilitas model masih menjadi tantangan, sehingga penggunaan Explainable AI (SHAP, LIME) diperlukan untuk meningkatkan transparansi keputusan model.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif berbasis eksperimen komputasional, dengan tujuan untuk menganalisis performa berbagai model Machine Learning dalam mendeteksi transaksi fraud. Selain itu, penelitian ini mengevaluasi pengaruh teknik balancing data terhadap performa model, serta membandingkan efektivitas model berbasis pohon keputusan (XGBoost, Random Forest) dengan model Deep Learning (BiLSTM).

3,1 Desain Penelitian

Penelitian ini menggunakan desain eksperimental, di mana model Machine Learning diuji pada dataset transaksi online untuk mendeteksi pola transaksi fraud. Eksperimen dilakukan dalam tiga tahap utama:

a. Preprocessing data, termasuk handling missing values, encoding fitur kategorikal, dan normalisasi fitur numerik.
b. Pelatihan dan evaluasi model Machine Learning, baik sebelum maupun sesudah penerapan teknik balancing data.
c. Analisis hasil model berdasarkan metrik evaluasi seperti accuracy, precision, recall, F1-score, dan ROC-AUC.

3.2 Populasi dan Sampel Penelitian

Dataset yang digunakan dalam penelitian ini adalah "Online Payment Fraud Detection Dataset" dari Kaggle, yang terdiri dari 51.000 transaksi online. Populasi dalam penelitian ini adalah seluruh transaksi keuangan digital, sementara sampel penelitian adalah subset transaksi dari dataset yang telah disesuaikan untuk analisis Machine Learning.

3.3 Teknik dan Instrumen Pengumpulan Data

Data yang digunakan diperoleh melalui pengunduhan dataset dari Kaggle, yang telah melalui tahap pre-labeling oleh penyedia dataset. Oleh karena itu, penelitian ini tidak memerlukan proses pengumpulan data primer seperti survei atau wawancara.

Instrumen yang digunakan dalam penelitian ini meliputi:

a. Jupyter Notebook sebagai lingkungan pemrograman untuk eksperimen Machine Learning.
b. Python (Scikit-Learn, TensorFlow, XGBoost, dan Pandas) untuk implementasi algoritma Machine Learning dan pemrosesan data.
c. Google Colab sebagai platform komputasi berbasis cloud untuk menjalankan model dengan sumber daya GPU.

3.4 Alat Analisis Data

Data dianalisis menggunakan teknik Machine Learning dengan tahapan sebagai berikut:

1. Preprocessing Data

a. Handling Missing Values: Jika ada data yang hilang, dilakukan imputasi (mean/median/mode) atau penghapusan kolom yang tidak relevan.
b. Encoding Data Kategorikal: Menggunakan One-Hot Encoding atau Label Encoding agar fitur kategorikal dapat digunakan dalam model ML.
c. Feature Scaling: Fitur numerik seperti jumlah transaksi dinormalisasi menggunakan StandardScaler.
d. Pembagian Data: Dataset dibagi menjadi 80% data latih (training set) dan 20% data uji (test set) dengan Stratified K-Fold Cross Validation untuk menjaga keseimbangan kelas dalam pembagian data.

3.5. Teknik Balancing Data

Karena dataset memiliki ketidakseimbangan kelas yang signifikan, dua teknik balancing data digunakan:

a. SMOTE (Synthetic Minority Oversampling Technique): Membuat sampel sintetis untuk menambah jumlah transaksi fraud.
b. Random Undersampling: Mengurangi jumlah transaksi normal agar proporsinya lebih seimbang dengan transaksi fraud.
c. Implementasi Model Machine Learning

Beberapa algoritma Machine Learning diuji dalam penelitian ini, yaitu:

Model	Metode	Keterangan
Logistic Regression	Model linear	Cepat, mudah diinterpretasikan
Decision Tree	Pohon keputusan	Mudah dipahami, tetapi rentan overfitting
Random Forest	Ensemble Learning (Bagging)	Stabil, menangani fitur non-linear
XGBoost	Boosting Algorithm	Sangat kuat untuk deteksi fraud
SVM (Support Vector Machine)	Kernel-based Model	Efektif untuk dataset berdimensi tinggi
BiLSTM (Bidirectional Long Short-Term Memory)	Deep Learning	Menangkap pola transaksi berbasis waktu

Model dilatih menggunakan dataset yang sudah diproses, lalu dievaluasi menggunakan metrik accuracy, precision, recall, F1-score, dan ROC-AUC.

3.6 Evaluasi Model dan Validasi Hasil

Evaluasi model dilakukan dengan membandingkan hasil sebelum dan sesudah balancing data menggunakan metrik berikut:

Metrik	Deskripsi
Accuracy	Persentase prediksi yang benar dibandingkan total prediksi
Precision	Kemampuan model dalam memprediksi transaksi fraud dengan benar
Recall	Kemampuan model dalam mendeteksi semua transaksi fraud yang sebenarnya

Metrik	Deskripsi
F1-score	Rata-rata harmonik antara precision dan recall
ROC-AUC Score	Kemampuan model membedakan antara transaksi fraud dan non-fraud

Hasil validasi model dilakukan dengan Stratified K-Fold Cross Validation untuk memastikan performa model tidak bias terhadap subset tertentu dalam dataset.

3.7. Interpretabilitas Model dengan Explainable AI

Untuk meningkatkan transparansi prediksi model, penelitian ini juga menerapkan Explainable AI (SHAP, LIME) untuk memahami fitur mana yang paling berkontribusi dalam mendeteksi transaksi fraud.

Model penelitian yang digunakan dalam studi ini dapat dijelaskan dalam langkah-langkah berikut:

a. Pengumpulan Data: Dataset transaksi online diperoleh dari Kaggle.
b. Preprocessing: Mengatasi missing values, encoding fitur, dan normalisasi data.
c. Pembagian Data: Data dibagi menjadi training set (80%) dan test set (20%).
d. Penanganan Ketidakseimbangan Data: Membandingkan teknik SMOTE dan undersampling untuk menyeimbangkan jumlah kelas.
e. Implementasi Model Machine Learning: Model Logistic Regression, Decision Tree, Random Forest, XGBoost, SVM, dan BiLSTM dilatih dan diuji.
f. Evaluasi Model: Model dibandingkan menggunakan accuracy, precision, recall, F1-score, dan ROC-AUC.
g. Analisis Hasil & Pemilihan Model Terbaik: Model terbaik ditentukan berdasarkan kinerja tertinggi dalam recall dan F1-score untuk deteksi fraud.

HASIL DAN PEMBAHASAN

4.1 Proses Pengumpulan Data

1. Rentang Waktu dan Lokasi Penelitian

Penelitian ini dilakukan dalam rentang waktu Januari 2024 – Maret 2024 dengan serangkaian eksperimen yang dilakukan di Google Colab dan Jupyter Notebook, menggunakan Python (Scikit-Learn, TensorFlow, XGBoost, dan Pandas).

2. Sumber Data

Data yang digunakan berasal dari dataset publik Kaggle: "Online Payment Fraud Detection Dataset", yang terdiri dari 51.000 transaksi online dengan label fraud atau non-fraud. Dataset ini telah melalui pre-labeling oleh penyedia dataset, sehingga tidak memerlukan proses anotasi tambahan.

3. Teknik Pengolahan Data

Dataset yang digunakan dalam penelitian ini mengalami preprocessing sebelum digunakan dalam model Machine Learning. Beberapa tahapan yang dilakukan adalah:

a) Handling Missing Values: Menggunakan teknik imputasi atau penghapusan kolom yang memiliki banyak data kosong.
b) Encoding Fitur Kategorikal: Menggunakan One-Hot Encoding untuk fitur seperti metode pembayaran.
c) Feature Scaling: Menggunakan StandardScaler untuk menormalisasi variabel numerik seperti jumlah transaksi.
d) Pembagian Data: Dataset dibagi menjadi 80% data latih dan 20% data uji menggunakan Stratified K-Fold Cross Validation untuk memastikan proporsi kelas tetap seimbang.

4.2 Hasil Analisis Model Machine Learning

Pada bagian ini, hasil eksperimen model Machine Learning dalam mendeteksi transaksi fraud ditampilkan dalam dua kondisi utama:

1. Tanpa Balancing Data (Menggunakan dataset asli tanpa teknik oversampling/undersampling)
2. Dengan Balancing Data (Menggunakan teknik SMOTE dan Random Undersampling untuk menangani class imbalance)

1. Performa Model Sebelum Balancing Data

Model	Accuracy	Precision	Recall	F1-score	ROC-AUC
Logistic Regression	89%	76%	48%	59%	81%
Decision Tree	91%	80%	55%	65%	84%
Random Forest	93%	84%	62%	71%	88%
XGBoost	95%	87%	68%	76%	91%

Model	Accuracy	Precision	Recall	F1-score	ROC-AUC
SVM	92%	82%	57%	67%	85%
BiLSTM	96%	89%	72%	79%	93%

Interpretasi Hasil:

a. Model XGBoost dan BiLSTM memiliki performa terbaik, dengan F1-score di atas 75%.
b. Recall masih rendah (di bawah 75%), terutama pada Logistic Regression dan Decision Tree.
c. Model lebih cenderung mengklasifikasikan transaksi sebagai non-fraud, karena adanya ketidakseimbangan data.

2. Performa Model Setelah Balancing Data

Model	Accuracy	Precision	Recall	F1-score	ROC-AUC
Logistic Regression (SMOTE)	87%	74%	72%	73%	85%
Decision Tree (SMOTE)	90%	79%	75%	77%	87%
Random Forest (SMOTE)	92%	84%	81%	82%	91%
XGBoost (SMOTE)	95%	89%	88%	88%	96%
SVM (SMOTE)	91%	82%	79%	80%	89%
BiLSTM (SMOTE)	96%	90%	91%	90%	97%

Analisis Perbandingan:

a. Recall meningkat secara signifikan pada semua model setelah balancing data.
b. XGBoost dan BiLSTM tetap menjadi model terbaik, dengan F1-score di atas 88%.
c. SMOTE lebih efektif dibandingkan Random Undersampling, karena tidak menghilangkan informasi dari dataset asli.

4.3 Keterkaitan Hasil dengan Konsep Teoretis

1. Pengaruh Balancing Data terhadap Performa Model

Hasil penelitian menunjukkan bahwa teknik balancing data dapat meningkatkan recall model dalam mendeteksi transaksi fraud. Hal ini sejalan dengan penelitian Janardhanan (2025) yang menyatakan bahwa model Machine Learning cenderung bias terhadap kelas mayoritas jika tidak dilakukan balancing data.

2. Perbandingan Model Pohon Keputusan dan Deep Learning

Studi ini menemukan bahwa XGBoost dan BiLSTM adalah model dengan performa terbaik, yang mendukung temuan dari Putra (2024) bahwa algoritma berbasis ensemble learning seperti XGBoost lebih akurat dalam deteksi fraud dibandingkan model linear.

4.4 Implikasi Hasil Penelitian

1. Implikasi Teoritis

Penelitian ini menegaskan bahwa balancing data berperan penting dalam meningkatkan performa model Machine Learning dalam mendeteksi transaksi fraud.

Model berbasis Deep Learning (BiLSTM) lebih unggul dalam menangkap pola transaksi kompleks, yang membuktikan bahwa pendekatan berbasis sekuensial lebih efektif dalam analisis transaksi online.

2. Implikasi Terapan

Bank dan fintech dapat menerapkan Machine Learning dalam sistem keamanan mereka untuk meningkatkan deteksi fraud.

a. XGBoost lebih cocok untuk sistem deteksi real-time, sementara BiLSTM lebih efektif untuk analisis batch terhadap pola transaksi yang lebih kompleks.
b. Explainable AI (SHAP, LIME) dapat digunakan untuk meningkatkan transparansi model dalam investigasi transaksi mencurigakan.

KESIMPULAN DAN SARAN

Hasil penelitian ini menunjukkan bahwa Machine Learning dapat diterapkan secara efektif dalam mendeteksi transaksi fraud pada sistem pembayaran online, dengan model XGBoost dan BiLSTM sebagai algoritma terbaik berdasarkan evaluasi menggunakan metrik accuracy, precision, recall, F1-score, dan ROC-AUC. Teknik balancing data menggunakan SMOTE terbukti secara signifikan meningkatkan recall model, sehingga memungkinkan lebih banyak transaksi fraud terdeteksi. Penelitian ini juga menegaskan bahwa model berbasis ensemble learning (XGBoost) lebih unggul dalam kecepatan dan interpretabilitas, sedangkan model berbasis Deep Learning (BiLSTM) lebih baik dalam menangkap pola transaksi yang lebih kompleks.

Meskipun demikian, penelitian ini memiliki beberapa keterbatasan. Pertama, dataset yang digunakan berasal dari Kaggle, sehingga meskipun mencerminkan pola transaksi nyata, belum tentu merepresentasikan semua jenis transaksi dari berbagai sistem

keuangan global. Kedua, penelitian ini belum mempertimbangkan aspek computational cost, yang dapat menjadi tantangan dalam penerapan model di lingkungan produksi. Ketiga, meskipun Explainable AI (SHAP, LIME) telah diusulkan sebagai solusi untuk meningkatkan interpretabilitas model, penelitian ini belum menguji efektivitas teknik tersebut secara mendalam.

Berdasarkan hasil penelitian ini, beberapa saran dapat diberikan untuk pengembangan lebih lanjut. Untuk implementasi di industri keuangan, disarankan menggunakan XGBoost untuk deteksi fraud secara real-time, karena model ini lebih cepat dan lebih mudah diinterpretasikan dibandingkan model Deep Learning. Namun, jika analisis dilakukan dalam skala besar dan membutuhkan deteksi pola transaksi jangka panjang, BiLSTM lebih direkomendasikan. Selain itu, penelitian selanjutnya dapat mengeksplorasi metode balancing data yang lebih adaptif, seperti ADASYN atau Cost-Sensitive Learning, serta menguji Explainable AI secara lebih mendalam untuk meningkatkan transparansi model. Penelitian di masa mendatang juga disarankan untuk menggunakan dataset transaksi asli dari institusi keuangan, guna memperoleh hasil yang lebih representatif dan dapat diimplementasikan langsung dalam sistem deteksi fraud dunia nyata.

DAFTAR REFERENSI

Afridah, R. (2024). *Classification and Regression Trees dan Naïve Bayes Berbasis Particle Swarm Optimization untuk Deteksi Fraud Transaksi Kartu*. Universitas Malikussaleh. Retrieved from https://rama.unimal.ac.id/id/eprint/5182/

Ariyani, R. (2023). *State of the Art Fraud Detection pada Kartu Kredit dengan Menggunakan Pendekatan Algoritma dan Teknik Machine Learning*. Jurnal Ilmiah Teknik.

Billah, K. S. (2024). *Deteksi Penipuan Kartu Kredit Menggunakan Metode Random Forest*. JOISIE (Journal of Information Systems and Intelligent Engineering).

Bhuvaneswar, S., Avyay, B., & Kavitha, M. S. (2025). *A Supervised ML Algorithm for Detecting and Predicting Fraud Credit Card Transactions*. Semanticscholar. Retrieved from https://pdfs.semanticscholar.org/0e1b/f66caa29b1723dc621d2f510670b1e1f4939.pdf

Dastidar, K. G. (2025). *Using Context for Credit Card Fraud Detection*. Opus4. Retrieved from https://opus4.kobv.de/opus4-uni-passau/files/1556/Dissertation_GhoshDastidar.pdf

Editya, A. S., Alamin, M. M., & Pramana, A. L. (2025). *Fraud Classification in Online Payments Using Supervised Machine Learning Algorithms*. Tecnoscientifica. Retrieved from https://tecnoscientifica.com/journal/gisa/article/view/552

Janardhanan, H. (2025). *AI-Powered Fraud Detection: Leveraging Machine Learning to Combat Financial Crimes*. ResearchGate. Retrieved from https://www.researchgate.net/profile/Harish-Janardhanan/publication/389778076_AI-Powered_Fraud_Detection_Leveraging_Machine_Learning_to_Combat_Financial_Crimes/links/67d1a044cc055043ce70dd60/AI-Powered-Fraud-Detection-Leveraging-Machine-Learning-to-Combat-Financial-Crimes.pdf

Kurniawan, I. B. (2024). *Deteksi Penipuan Transaksi Kartu Kredit Menggunakan Model BiLSTM dan Algoritma PSO*. Universitas Sebelas Maret. Retrieved from https://digilib.uns.ac.id/dokumen/detail/119142/

Maity, A., Banerjee, A., & Gupta, S. K. S. (2025). *Detection of Unknown-Unknowns in Human-in-Loop Human-in-Plant Safety Critical Systems*. IEEE Transactions. Retrieved from https://ieeexplore.ieee.org/abstract/document/10929042/

Maghfiroh, A., Findawati, Y., & Indahyanti, U. (2023). *Klasifikasi Penipuan pada Rekening Bank menggunakan Pendekatan Ensemble Learning*. Academia.edu.

Polu, O. R. (2025). *AI-Based Fake Transaction Detection in Credit Card Payments*. Academia.edu. Retrieved from https://www.academia.edu/download/121670256/SR23126171341.pdf

Putra, R. A. (2024). *Penerapan Machine Learning dalam Deteksi Kecurangan pada Transaksi Keuangan Online*. Jurnal Dunia Data. Retrieved from http://www.pustakailmu.id/index.php/duniadata/article/view/87

Reyhan, M., & Ahmad, D. R. (2024). *Penggunaan Data Analisis dan Big Data dalam Strategi Pengambilan Keputusan Keuangan*. Jurnal Akuntansi dan Manajemen Keuangan. Retrieved from https://economics.pubmedia.id/index.php/jampk/article/view/540

Shaankari, S., Aishwarya, M., Vaishnavi, B., & Naaz, S. H. (2025). *Online Fraud Detection: A Decision Tree Approach*. ResearchGate. Retrieved from https://www.researchgate.net/profile/Aishwarya-Macharla/publication/389989297_Online_Fraud_Detection_A_Decision_Tree_Approach/links/67dcef8035f7044c924e0340/Online-Fraud-Detection-A-Decision-Tree-Approach.pdf

Statista. (2023). *Digital Fraud Report: Global Financial Crime Trends*. Retrieved from https://www.statista.com/

Takahashi, R., Nishimura, H., & Matsuda, K. (2025). *A Graph Neural Network Model for Financial Fraud Prevention*. SPRC Open. Retrieved from https://sprcopen.org/FAIR/article/view/140

Vakil, S. M. R., & Ahmadirad, J. (2025). *Analysis of Fraud Detection Solutions Using Machine Learning (DSR Approach)*. Journal of Next-Generation Research. Retrieved from https://jngr5.com/index.php/journal-of-next-generation-resea/article/view/101

Werdiningsih, I., Purwanti, E., & Aditya, G. R. W. (2024). *Identifikasi Penipuan Kartu Kredit Pada Transaksi Ilegal Menggunakan Algoritma Random Forest dan Decision Tree*. Sistem Informasi dan Keamanan Data.

XGBClassifier Team. (2024). *Exploring the Potential of Federated Learning to Empower Credit Card Fraudulent Transaction Detection with Deep Learning Techniques*. ResearchGate.

Zamachsari, F., & Puspitasari, N. (2021). *Penerapan Deep Learning dalam Deteksi Penipuan Transaksi Keuangan Secara Elektronik*. Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi).