Vol. 4 No. 2 – Tahun 2025
Indonesian Journal Computer Science
ISSN: 2829-3819

Optimasi Deteksi Penipuan Kartu Kredit Menggunakan Regresi Logistik dengan Particle Swarm Optimization

Icha Nura Nugraha [1], David Dos Santos Pinto Lopes [2], Muhammad Hanafi [3]
Universitas Amikom Yogyakarta,[1,2,3]
ichanugraha@students.amikom.ac.id [1], dossantosdavid@students.amikom.ac.id [2],
hanafi@amikom.ac.id [3]

Diterima	Direvisi	Disetujui
(28-05-2025)	(14-07-2025)	(06-08-2025)

Abstrak - Meningkatnya prevalensi transaksi digital telah menyebabkan lonjakan penipuan kartu kredit, yang memerlukan metode deteksi canggih yang menyeimbangkan akurasi dan efisiensi komputasi. Studi penelitian mengusulkan sistem deteksi penipuan yang dioptimalkan menggunakan Logistic Regression (LR) dengan Particle Swarm Optimization (PSO). Peran untuk mengatasi tantangan ketidakseimbangan kelas dan data berdimensi tinggi, kerangka kerja tersebut menggabungkan Teknik Oversampling Minoritas Sintetis (SMOTE) untuk penyeimbangan data, RobustScaler untuk normalisasi yang tahan terhadap outlier, dan Analisis Komponen Utama (PCA) untuk pengurangan dimensionalitas. Algoritma PSO mengoptimalkan parameter LR (C), meningkatkan generalisasi model dan kinerja deteksi. Eksperimen dilakukan pada kumpulan data Credit Card yang berisi 284.807 transaksi, dengan kasus penipuan hanya mewakili 0,172% dari data ketidakseimbangan kelas yang parah. Model yang diusulkan mencapai akurasi 97,47%, presisi 99,82%, recall 89% (kelas penipuan), dan skor ROC-AUC 0,97, yang menunjukkan kinerja yang unggul dalam membedakan transaksi penipuan. Matriks kebingungan mengungkapkan 110 positif benar (deteksi penipuan yang benar) dengan hanya 13 negatif palsu, yang menunjukkan identifikasi penipuan yang kuat sekaligus meminimalkan alarm palsu. Analisis komparatif di berbagai pemisahan pengujian mengonfirmasi konsistensi model, dengan F1-Score secara konsisten di atas 98,5%. Hasil tersebut menyoroti efektivitas penyetelan hiperparameter berbasis PSO dalam meningkatkan kinerja LR, khususnya dalam kumpulan data yang tidak seimbang. Integrasi SMOTE dan PCA memastikan efisiensi komputasi tanpa mengorbankan kemampuan deteksi. Pendekatan memberi solusi yang dapat diskalakan dan presisi tinggi untuk deteksi penipuan waktu nyata, mengurangi kerugian finansial sekaligus mempertahankan efisiensi operasional.

Kata Kunci : Logistic Regression, Particle Swarm Optimization, PCA, Penipuan Kartu Kredit, SMOTE.

Abstract *- The increasing prevalence of digital transactions has led to credit card fraud, which requires advanced detection methods that balance accuracy and computational efficiency. The research study proposes an optimized fraud detection system using Logistic Regression (LR) with Particle Swarm Optimization (PSO). Serving to address the challenges of class synchronization and high-dimensional data, the framework combines Synthetic Minority Oversampling Technique (SMOTE) for data balancing, RobustScaler for outlier-robust normalization, and Principal Component Analysis (PCA) for dimensionality reduction. The PSO algorithm optimizes the LR regularization parameter (C), improving model generalization and detection performance. Experiments are conducted on a Credit Card dataset containing 284,807 transactions, with fraud cases representing only 0.172% of the data to the severe class performance. The proposed model achieves 97.47% accuracy, 99.82% precision, 89% recall (fraud class), and a ROC-AUC score of 0.97, indicating superior performance in distinguishing fraudulent transactions. The confusion matrix revealed 110 true positives (correct fraud detections) with only 13 false negatives, indicating robust fraud identification while minimizing false alarms. Comparative analysis across multiple model consistency testing verifies, with F1-Score consistently above 98.5%. The results highlight the effectiveness of PSO-based hyperparameter tuning in improving LR performance, especially in imbalanced datasets. The integration of SMOTE and PCA ensures computational efficiency without sacrificing detection capability. The approach provides a scalable and high-precision solution for real-time fraud detection, reducing financial losses while maintaining operational efficiency.*

Keywords: Credit Card Fraud, Logistic Regression, Particle Swarm Optimization, PCA, SMOTE.

I. PENDAHULUAN

Proses aktivitas dilakukan melalui internet membuat hidup menjadi lebih mudah dan efisien. Kasus penipuan yang menyebabkan seseorang mengalami kerugian finansial adalah salah satu dari banyak masalah yang sering dialami pada era digitalisasi (Madhurya et al., 2022). Mengidentifikasi transaksi kartu kredit penipuan secara efisien dan akurat menjadi perhatian global yang signifikan (Knn & Regression, 2023). Eksplorasi dalam deteksi penipuan kartu kredit menggunakan teknik machine learning sudah pernah dilakukan (Madhurya et al., 2022) & (Bin Sulaiman et al., 2022). Ekplorasi penting dan perlu untuk dilakukan seperti melakukan optimasi. Swarm optimasi mengalami perkembangan sejak tahun enam puluh (Ab Wahab et al., 2015). Meningkatnya volume transaksi keuangan, penipuan semakin sulit di deteksi. Maka perlu adanya optimasi dalam evaluasi dan penerapan yang optimal.

Scaling adalah himpunan data, scaling juga dikenal sebagai normalisasi merupakah langkah preprocessing yang penting dalam alur machine learning (de Amorim et al., 2023). Scaling merupakan metode normalisasi yang populer, robustscaler merupakan metode teknik scaling yang mampu menghadapi data dengan outlier. Tingginya ketersediaan data menjadi sebab utama yang dapat menimbulkan adanya outlier. Usulan penggunaan scaling diterapkan pada metode yang digunakan. Tingginya data memberikan tingkat komputasi yang tinggi, dalam usulan yang diterapkan *Principal Component Analysis* (PCA) diterapkan untuk menekan komputasi agar komsumsi memori dan komputasi dapat maksimal (Bansal & Garg, 2021).

Penelitian dalam pendekatan froud of detection dalam mendeteksi sering kali menggunakan metode SMOTE untuk menyeimbangkan data (Alatawi, 2025) & (Afriyie et al., 2023). Dalam kasus untuk deteksi Penipuan Kartu Kredit sering kali berbagai penelitian bahkan melakukan komparasi antara metode yang lain. Penerapan regresi logistik digunakan beberapa penelitian untuk memodelkan probabilitas penipuan kartu kredit (Kilickaya, 2024). Berdasarkan pendahuluan terdahulu bahwa terdapat beberapa hal perlu untuk dilakukan evaluasi lebih lanjut dalam hal prediksi terkait penipuan kartu kredit yang sering terjadi.

Pendekatan meliputi beberapa aspek terkait pendekatan yang diusulkan berdasarkan penelitian terdahulu dan teori kajian untuk memuat pendekatan Perbandingan dan analisis regresi logistic (Itoo et al., 2021). diterapkan dalam algoritma pembelajaran mesin untuk deteksi penipuan kartu kredit. Kinerja algoritma ini direkomendasikan dengan analisis komparatif. Pekerjaan ini diimplementasi menggunakan bahasa python dan kinerja algoritma diukur berdasarkan akurasi, sensitivitas, spesifisitas, presisi, F1 score, dan luas di bawah kurva. Data yang tidak seimbang atau miring diproses sebelumnya dengan teknik pengambilan sampel ulang (pengambilan sampel berlebihan atau pengambilan sampel kurang) untuk hasil yang lebih baik (Itoo et al., 2021) Optimization menggunakan algoritma logistic regression (Hussein et al., 2021)

Optimasi menggunakan logistik regression dalam prediksi gabungan menjadi input data untuk meta yang diusulkan adalah peran yang merupakan regresi logistik untuk menghasilkan hasil prediktif akhir dalam deteksi yang lebih baik. Hasil simulasi dibandingkan dengan tujuh algoritma lainnya menegaskan bahwa model ansambel dapat mendeteksi penipuan kartu kredit secara memadai dengan tingkat deteksi 84,90% dan 76,30% (Hussein et al., 2021). dalam penelitian yang diterapkan. visualisasi model regresi logistik, langkah penting dalam menilai efektivitasnya adalah penciptaan kurva *Receiver Operating Characteristic* (ROC) (Kilickaya, 2024) dimana hal tersebut Kemampuan model regresi logistik untuk menyeimbangkan sensitivitas dan spesifisitas.

Menerapkan model regresi logistik fuzzy yang kuat terhadap ketidakseimbangan kelas dan masalah pemisahan, kami mengatasi tantangan memiliki tingkat transaksi penipuan yang sangat rendah dalam kumpulan data dan memiliki masalah pemisahan karena karakteristik transaksi tertentu dalam scaling (Charizanos et al., 2024) logistic regression yang dihasilkan 97.7% akurasi (Afriyie et al., 2023). Efektivitas kriteria meliputi eksperimen dengan kumpulan data yang tidak seimbang secara signifikan. Pendekatan ini dapat di manfaatkan dalam penerapan alur yang di usulkan sebagai celah identifikasi untuk dapat diterapkan.

Makalah pendekatan yang diusulan dalam penelitian dalam prediksi terkait penipuan meliputi terkait studi kasus sebelumnya dalam penekanan peran tersebut. Dalam rangkuman paper yang dibuat dapat disimpulkan lebih detail meliputi point dua literature review yang terdiri dari hubungan dari penelitian sebelumnya dan juga terdiri dari landasan teori dalam penegasan penggunaan metode yang diusulkan. Langkah ketiga merupakan pembahasan dari metode yang diusulkan dalam pendekatan sehingga

dapat menjadi kesimpulan yang menjadikan implikasi untuk penelitian selanjutnya.

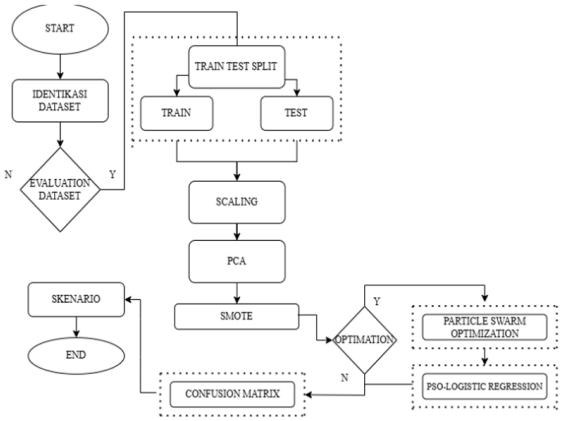
II. METODOLOGI PENELITIAN

Metodologi dalam pendekatan prediksi yang digunakan dalam penelitian ini secara terperinci dapat dijelaskan melalui Gambar 1. tersebut menggambarkan secara sistematis alur kerja penelitian yang diusulkan, dimulai dari tahap awal yaitu identifikasi dan evaluasi dataset. Evaluasi dilakukan untuk memastikan bahwa dataset yang digunakan memenuhi kriteria kualitas dan kelayakan untuk pemodelan. Setelah proses evaluasi, dataset kemudian dibagi menjadi dua bagian utama, yakni 80% data digunakan sebagai data pelatihan (training) dan sisanya 20% digunakan sebagai data pengujian (testing). Pembagian ini bertujuan untuk memastikan bahwa model yang dikembangkan dapat diuji secara valid terhadap data yang belum pernah dilihat sebelumnya, sehingga performa model dapat dinilai secara objektif.

Tahapan selanjutnya adalah proses prapemrosesan data, salah satunya dengan menerapkan teknik skaling menggunakan Robust Scaler. Teknik dipilih karena memiliki kemampuan dalam mengurangi pengaruh outlier atau nilai-nilai ekstrem yang dapat memengaruhi performa algoritma pembelajaran mesin. Robust Scaler memberikan nilai tambah dalam menjaga stabilitas model yang dihasilkan, terutama pada data yang tidak terdistribusi normal. Setelah proses scaling, dilakukan penerapan metode *Principal Component Analysis* (PCA). PCA digunakan untuk mereduksi dimensi data, sehingga dapat mengurangi kompleksitas komputasi dan beban memori tanpa mengorbankan informasi penting dari fitur asli. Langkah ini sangat penting terutama ketika berhadapan dengan data berdimensi tinggi.

Pendekatan juga melibatkan teknik *Synthetic Minority Over-sampling Technique* (SMOT *E (Synthetic Minority Over-sampling Technique)* yang memiliki peran krusial dalam menangani ketidakseimbangan kelas dalam dataset. Dalam banyak kasus deteksi penipuan kartu kredit, jumlah data transaksi normal jauh lebih besar dibandingkan transaksi penipuan, sehingga berpotensi menyebabkan bias dalam pembelajaran model. Penerapan SMOTE bertujuan untuk menyeimbangkan proporsi kelas mayoritas dan minoritas dengan cara mensintesis data baru pada kelas minoritas, sehingga model tidak hanya fokus pada kelas mayoritas dan dapat mempelajari pola penipuan dengan lebih baik.

Langkah terakhir dalam metodologi adalah proses optimasi parameter menggunakan algoritma *Particle Swarm Optimization* (PSO). PSO digunakan untuk menemukan kombinasi parameter terbaik dari model yang akan dibangun, dalam hal ini algoritma Logistic Regression. PSO bekerja dengan meniru perilaku sosial sekumpulan partikel dalam mencari solusi optimal dari sebuah permasalahan. Setelah parameter optimal diperoleh, model Logistic Regression dilatih dengan dataset yang telah diproses sebelumnya. Untuk mengevaluasi performa model, digunakan metrik evaluasi yang diperoleh dari confusion matrix seperti akurasi, presisi, recall, dan F1-score. Evaluasi ini bertujuan untuk mengetahui seberapa baik model mampu memprediksi transaksi yang termasuk dalam kategori penipuan maupun tidak.

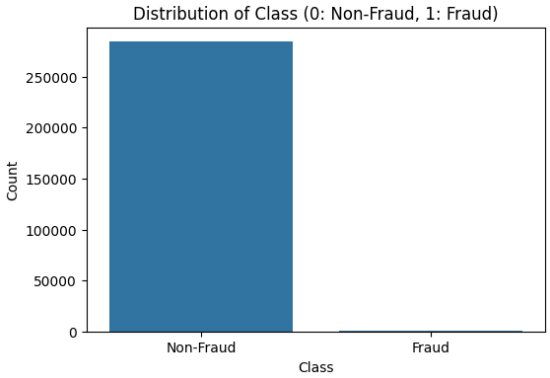


Sumber: Hasil Penelitian Penulis (2025).

Gambar 1. Diagram Alir Penelitian

1. Dataset

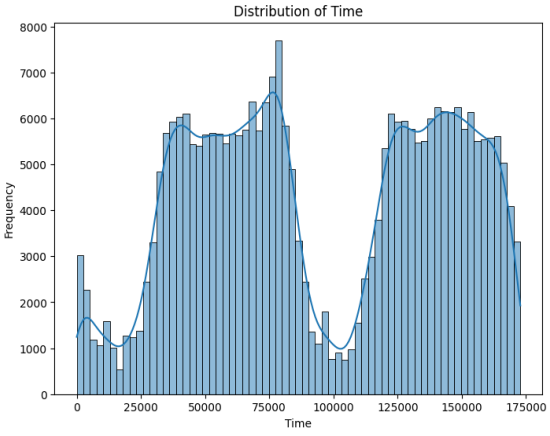
Dataset (Alarfaj et al., 2022), bersumber dari kaggle terdiri dari variable time, v1 hingga v28, Amout dan Class. Data Credit Card Fraud berjumlah 284807 rows × 31 columns. Data tersebut dapat dilihat berdasarkan nilai distribusi kelas dan distribusi waktu yang direpresentasikan pada gambar 2 dan 3 tersebut akan menjelaskan secara detail seberapa baik data direpresentasikan ke dalam grafik bar. Pada gambar 2 menjelaskan distribusi class yang teridentifikasi non-fraud dan fraud, representasi nilai numerik sebagai identifikasi nilai biner 0 dan 1 dalam menentukan class pada distribusi nilai dataset credit card. Dalam grafik gambar 2 juga dapat menerangkan bahwa terdapat data yang tidak seimbang.



Sumber: Hasil Penelitian Penulis (2025).

Gambar 2. Distribusi Class Fraud and Non-Fraud

Frekuensi jumlah waktu mengalami kenaikan secara drastic dan menurun secara drastic lau waktu mengalami kestabilan pada rentang 12500. Distribusi ini dapat menurun dipertengah ada indicator mencurigakan dalam sektor waktu yang berdekatan. Peran identifikasi ini dapat dan juga tidak digunakan dalam pertimbagan penelitian yang di usulkan.



Sumber: Hasil Penelitian Penulis (2025).

Gambar 3. Distribusi Time Credit Card Fraud

2. Prepreprocessing Identifikasi

Preprocessing diterapkan dalam penerapan usulan dari metode yang diterapkan. Missing value menyebabkan ketidak fungsian dari sebuah mesin dalam mempelajari data dengan baik. Preprocessing berperan penting dalam metode yang diusulkan. Menghilangkan noise secara konsisten dapat membuktikan hasil model yang lebih akurat. Normalisasi dapat diterapkan dengan cara fitur numerik dalam dataset dinormalisasi menggunakan metode StandardScaler untuk memastikan bahwa semua fitur memiliki skala yang seragam. Proses normalisasi ini dilakukan dengan cara mengubah nilai setiap fitur sehingga memiliki rata-rata 0 dan standar deviasi 1.

Langkah ini bertujuan untuk mengurangi dampak perbedaan skala antar fitur yang dapat memengaruhi performa model. Sehinga model dapat memproses data lebih efisien dan mencapai konvergensi lebih cepat selama pelatihan sehingga meningkatkan akurasi dan stabilitas hasil prediksi. Menghadapi masalah ketidak seimbangan kelas yang terdapat dalam dataset, digunakan metode *Synthetic Minority Oversampling Technique* (SMOTE) sebagai solusi. Ketidakseimbangan kelas ini biasanya terjadi ketika jumlah sampel pada salah satu kelas, seperti kelas minoritas, jauh lebih sedikit dibandingkan kelas mayoritas. Dalam konteks ini, kelas minoritas yang dimaksud adalah data yang berkaitan dengan kasus penipuan. SMOTE bekerja dengan cara mensintesis sampel-sampel baru yang dihasilkan dari data yang sudah ada pada kelas minoritas.

3. Penerapan Algoritma

Principal Component Analysis (PCA). Pengaturan PCA dalam eksperimen menggunakan parameter n_components sebesar 0.95, yang berarti hanya komponen yang mencakup 95% dari total variansi data akan dipertahankan. Sedangkan ketidak seimbangan kelas dalam dataset diatasi menggunakan *Synthetic Minority Oversampling Technique* (SMOTE), yang menghasilkan sampel tambahan untuk kelas minoritas guna menciptakan distribusi kelas yang lebih seimbang. *Particle Swarm Optimization* (PSO) Parameter yang dioptimalkan adalah nilai regularisasi C, dengan batas pencarian diatur antara 0.01 hingga 10. Report, ROC-AUC Score, dan Confusion Matrix, yang memberikan wawasan tentang performa model pada data uji untuk memberikan analisis yang lebih mendalam, fungsi tambahan disediakan untuk menghitung metrik seperti Precision, Recall, F1-Score, dan Accuracy dalam format persentase.

4. Evaluasi Metrik

Evaluasi dalam machine learning yang digunakan untuk menganalisis performa mode Matriks ini menunjukkan perbandingan antara prediksi model dengan label sebenarnya dari data.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \qquad (3.1)$$

Metrik yang mengukur proporsi prediksi yang benar dari keseluruhan data Akurasi

menunjukkan seberapa baik model secara keseluruhan dalam membuat prediksi yang benar.

$$Precision = \frac{TP}{FP + TP} \quad (3.2)$$

Metrik yang mengukur proporsi prediksi positif yang benar dari semua prediksi yang dianggap positif oleh model. Presisi menilai seberapa tepat model saat memprediksi kelas positif, dengan meminimalkan jumlah.

$$Recall = \frac{TP}{FN + TP} \quad (3.3)$$

Metrik yang mengukur proporsi data kelas positif yang berhasil dideteksi dengan benar oleh model Recall menilai seberapa baik model dalam menemukan semua data positif, dengan meminimalkan False Negative.

$$F1 - Score = 2x\frac{precision\ x\ recall}{precision + recall} \quad (3.4)$$

Rata-rata harmonis antara presisi dan recall, memberikan keseimbangan antara kedua metrik tersebut. F1-Score berguna ketika kita ingin mempertimbangkan baik presisi maupun recall, terutama pada dataset yang tidak seimbang.

III. HASIL DAN PEMBAHASAN

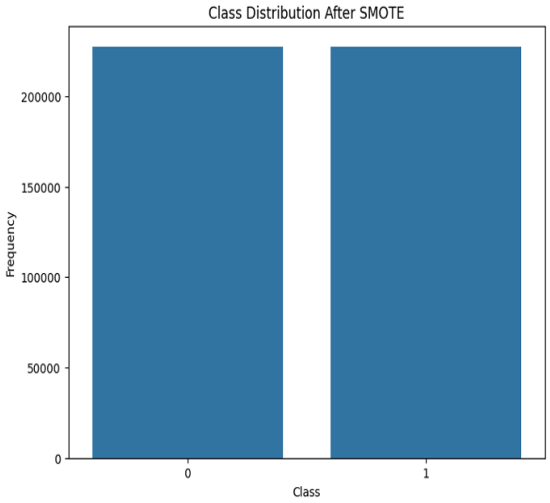
Hasil Salah satu metode yang digunakan dalam model dalam penelitian ini adalah model regresi Logistik (Ileberi et al., 2022), Metode regresi logistik adalah pendekatan pembelajaran mesin yang populer dan sederhana (Afriyie et al., 2023). Proses deteksi penipuan (FDP) dan proses pencegahan penipuan (FPP) (Razaque et al., 2023). dalam kegunaanya metode regresi lebih unggul dalam penanganan dalam fraud detection.

Particle Swarm Optimization (PSO) adalah teknik optimasi yang diperkenalkan oleh Kennedy dan Eberhart pada tahun 1995. Ini menggunakan mekanisme sederhana yang meniru perilaku kawanan burung dan sekolah ikan untuk memandu partikel untuk mencari solusi optimal global Algoritma PSO dimulai dengan menginisialisasi populasi terlebih dahulu. Langkah kedua adalah menghitung nilai kesesuaian setiap partikel, diikuti dengan memperbarui yang terbaik individu dan global, dan kemudian, kecepatan dan posisi partikel diperbarui (Ab Wahab et al., 2015).

SMOTE peran dalam penerapan bekerja dengan memilih objek yang terletak dekat di bagian fitur, berharap untuk mendapatkan garis di antara objek-objek, dan kemudian menghasilkan kumpulan data baru di bagian yang dihimpun. Penerapan secara instance acak dari kelas minoritas dipilih, dan proses ini dapat diulangi untuk menghasilkan instance sintetis sebanyak mungkin untuk kelas minoritas sesuai kebutuhan. Metodologi ini terbukti efektif karena menghasilkan instance sintetis yang masuk akal, sangat mirip dengan instance yang ada dari kelas minoritas di ruang fitur (Yan et al., 2024).

1. Handle Balance Data

Gambar (4) adalah sebuah histogram yang menunjukkan distribusi kelas setelah penerapan metode *Synthetic Minority Oversampling Technique* (SMOTE). Pada grafik tersebut, sumbu horizontal (x-axis) merepresentasikan label kelas, yaitu 0 dan 1, sedangkan sumbu vertikal (y-axis) menunjukkan frekuensi atau jumlah data pada masing-masing kelas. Setelah penerapan SMOTE, distribusi data terlihat seimbang dengan jumlah data pada kedua kelas yang hampir sama, yaitu sekitar 200.000 untuk kelas 0 dan kelas 1. Hal ini menunjukkan bahwa metode SMOTE berhasil menyeimbangkan jumlah data antara kelas mayoritas (kelas 0) dan minoritas (kelas 1) dengan menciptakan sampel sintetis pada kelas minoritas.



Sumber: Hasil Penelitian Penulis (2025).

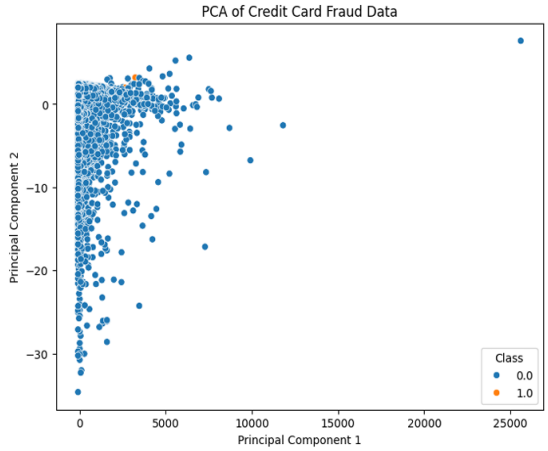
Gambar 4. SMOTE CLASS Distribusi

SMOTE membuktikan teknik yang umum digunakan dalam pemrosesan data untuk mengatasi masalah ketidak seimbangan kelas pada dataset. Ketidakseimbangan kelas dapat menyebabkan algoritma pembelajaran mesin bias terhadap kelas mayoritas, sehingga menurunkan performa prediksi pada kelas minoritas. Dengan menciptakan data sintetis pada kelas minoritas, SMOTE meningkatkan

peluang model untuk belajar pola yang lebih representatif dari kedua kelas secara seimbang. Histogram ini mencerminkan hasil dari proses tersebut, di mana kini kedua kelas memiliki jumlah data yang setara, sehingga model yang dilatih dengan dataset ini diharapkan mampu melakukan prediksi yang lebih adil dan akurat.

2. Principal Component analisis dan PSO

Gambar (5) adalah scatter plot yang menggambarkan distribusi data dari sebuah dataset penipuan kartu kredit setelah direduksi menggunakan teknik PCA (Principal Component Analysis). Sumbu horizontal (x-axis) menunjukkan nilai dari komponen utama pertama (Principal Component 1), sedangkan sumbu vertikal (y-axis) menunjukkan nilai dari komponen utama kedua (Principal Component 2). Titik-titik biru mewakili data kelas 0 (non penipuan), sedangkan titik-titik oranye mewakili data kelas 1 (penipuan). Grafik ini digunakan untuk memvisualisasikan data dalam ruang berdimensi rendah (2 dimensi) guna memahami pola distribusi data, terutama untuk melihat apakah ada perbedaan pola yang signifikan antara kedua kelas.

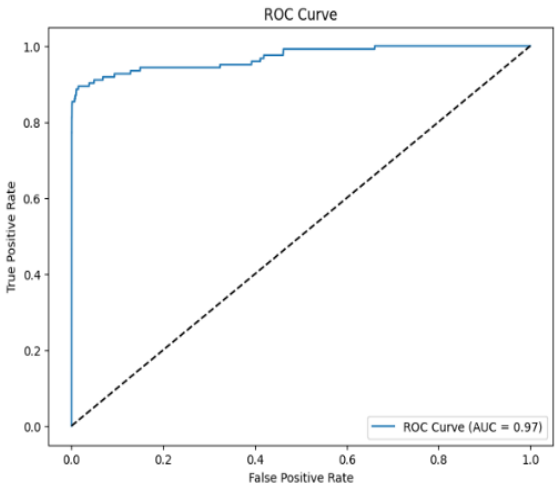


Sumber: Hasil Penelitian Penulis (2025).

Gambar 5. PCA Credit Card Fraud

Berdasarkan visualisasi plot gambar (5), terlihat bahwa sebagian besar data berada di sekitar nilai nol pada Principal Component 2 dan cenderung terkonsentrasi di sisi kiri pada Principal Component 1. Kelas penipuan (kelas 1) hanya diwakili oleh sedikit titik oranye dan tampak tumpang tindih dengan data kelas non-penipuan (kelas 0). Hal ini menunjukkan bahwa data penipuan sangat jarang (imbalance), serta sulit dibedakan dari data non-penipuan hanya dengan melihat dua komponen utama. PCA (Leevy et al., 2023) membantu mengidentifikasi struktur data, tetapi untuk dataset seperti ini, diperlukan algoritma pembelajaran mesin yang lebih canggih untuk mendeteksi pola-pola kompleks yang memisahkan kedua kelas.

Gambar di atas merupakan kurva ROC (Receiver Operating Characteristic) yang digunakan untuk mengevaluasi performa model klasifikasi biner. Sumbu horizontal (x-axis) menunjukkan tingkat False Positive Rate (FPR), yang mengukur proporsi data negatif yang secara keliru diklasifikasikan sebagai positif. Sumbu vertikal (y-axis) menunjukkan True Positive Rate (TPR), yang merupakan proporsi data positif yang benar-benar diklasifikasikan sebagai positif. Kurva biru menunjukkan hubungan antara TPR dan FPR pada berbagai ambang batas klasifikasi, sementara garis putus-putus (diagonal) merepresentasikan kinerja model acak (AUC = 0.5) , yang berfungsi sebagai baseline.



Sumber: Hasil Penelitian Penulis (2025).

Gambar 6. Receiver Operating Characteristic

Nilai AUC (Area Under the Curve) (Ileberi et al., 2021) pada grafik ini adalah 0.97, yang menunjukkan performa model yang sangat baik. Semakin mendekati nilai 1, semakin baik kemampuan model untuk membedakan antara kelas positif dan negatif. Bentuk kurva yang melengkung tajam ke arah sudut kiri atas mengindikasikan bahwa model mampu mencapai TPR yang tinggi dengan tingkat FPR yang rendah. Dengan kata lain, model memiliki kemampuan prediksi yang sangat akurat, terutama dalam mendeteksi data positif (misalnya, kasus penipuan). Namun, interpretasi ini perlu dipadukan dengan metrik lain seperti presisi dan recall untuk memastikan keseimbangan kinerja model pada data yang tidak seimbang.

3. Hasil Evaluasi Metrix

Hasil evaluasi performa model dalam mendeteksi penipuan kartu kredit. Metode yang digunakan menghasilkan nilai ROC-AUC Score sebesar 0,97, yang mencerminkan kemampuan model dalam membedakan antara kelas penipuan (1) dan non-penipuan (0). Matriks klasifikasi menunjukkan bahwa model berhasil mengklasifikasikan 69.288 data transaksi non-penipuan dengan benar (True Negative) dan hanya salah mengklasifikasikan 1.791 transaksi sebagai penipuan (False Positive). Untuk data penipuan, model berhasil mendeteksi 110 transaksi dengan benar (True Positive), tetapi ada 13 transaksi yang tidak terdeteksi sebagai penipuan (False Negative).

Evaluasi tersebut dapat juga similar dengan kondisi yang ada pada tabel komparasi data train yang digunakan untuk mencari nilai akurasi paling terbaik. Dimana hal tersebut dapat di amati secara lengkap hasil dari komparasi yang dihasilkan dari metode optimasi. Dalam kasus tersebut akurasi paling rendah dihasilkan pada 97,38% yang dilengkapi dan diteruskan pada akurasi tertinggi pada gambar.

```
              precision    recall  f1-score   support

           0       1.00      0.97      0.99     71079
           1       0.06      0.89      0.11       123

    accuracy                           0.97     71202
   macro avg       0.53      0.93      0.55     71202
weighted avg       1.00      0.97      0.99     71202

ROC-AUC Score: 0.9721991458719298

Confusion Matrix:
[[69288  1791]
 [   13   110]]

Model Performance Metrics (in %):
Precision: 99.82%
Recall: 97.47%
F1-Score: 98.56%
Accuracy: 97.47%
```

Sumber: Hasil Penelitian Penulis (2025).

Gambar 7. Confusion Matrix

Hasil gambar (7) evaluasi metrik kinerja menunjukkan bahwa model memiliki tingkat akurasi sebesar 97,47% dan presisi sebesar 99,82%, yang berarti hampir semua prediksi positif yang diberikan model adalah benar. Recall pada kelas penipuan tercatat 89%, mengindikasikan bahwa meskipun model sangat akurat untuk mendeteksi kelas mayoritas (non penipuan), model masih dapat mendeteksi sebagian besar kasus penipuan. Dengan F1-score sebesar 98,56%, model menunjukkan keseimbangan antara presisi dan recall, menjadikannya efektif untuk digunakan dalam aplikasi nyata, terutama dalam konteks mendeteksi kasus penipuan yang memiliki data tidak seimbang dibandingkan dengan (Afriyie et al., 2023) dan lebih komprehensif (Dornadula & Geetha, 2019).

Tabel 1. Komparasi Skenario

Data Test	Logistic Regression PSO				
	Accuracy	Precision	Recall	F1-Score	ROC
20	97,38%	99,82%	97,38%	98,52%	0,97
22	97,45%	99,82%	97,45%	98,55%	0,97
25	97,47%	99,82%	97,47%	98,56%	0,97

Sumber: Hasil Penelitian Penulis (2025).

Berdasarkan data tabel (1) hasil evaluasi model Logistic Regression yang dioptimasi menggunakan PSO, performa model menunjukkan hasil yang konsisten dan sangat baik di berbagai uji dengan data test. Akurasi model berada pada kisaran tinggi, yaitu 97,38% hingga 97,47%, menunjukkan bahwa model mampu membuat prediksi yang benar dalam sebagian besar kasus. Presisi model mencapai 99,82% secara konsisten, menandakan tingkat kesalahan prediksi positif sangat rendah.

Berdasarkan data tabel (1) hasil evaluasi model Logistic Regression yang dioptimasi menggunakan PSO, performa model menunjukkan hasil yang konsisten dan sangat baik di berbagai uji dengan data test. Akurasi model berada pada kisaran tinggi, yaitu 97,38% hingga 97,47%, menunjukkan bahwa model mampu membuat prediksi yang benar dalam sebagian besar kasus. Presisi model mencapai 99,82% secara konsisten, menandakan tingkat kesalahan prediksi positif sangat rendah.

IV. KESIMPULAN

Pendekatan yang diusulkan berhasil memberikan hasil yang cukup baik dan meningkat setiap proses pengujian pada performa deteksi penipuan kartu kredit yang dihasilkan, seperti dibuktikan dengan akurasi hingga 97,47%, precision 99,82%, F1-Score 98.56%, recall 97,47% dan nilai ROC-AUC sebesar 0,97. SMOTE berperan penting dalam mengatasi ketidakseimbangan data, sementara Robust Scaler dan PCA membantu dalam preprocessing data. Optimasi Logistic Regression dengan PSO memberikan hasil yang lebih akurat dibandingkan metode lainnya. Solusi ini efektif dalam menangani dataset besar dengan ketidakseimbangan kelas dan dapat

diadaptasi untuk implementasi lebih lanjut dalam kasus-kasus serupa. Implikasi masa depan dapat menggunakan komparasi skaling lain seperti standarscaling, explorasi dengan parameter yang lebih baik. Optimasi seperti Generatif dalam optimasi optimal.

V. REFERENSI

Ab Wahab, M. N., Nefti-Meziani, S., & Atyabi, A. (2015). A comprehensive review of swarm optimization algorithms. PLoS ONE, 10(5), 1–36. https://doi.org/10.1371/journal.pone.0122827

Afriyie, J. K., Tawiah, K., Pels, W. A., Addai-Henne, S., Dwamena, H. A., Owiredu, E. O., Ayeh, S. A., & Eshun, J. (2023). A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. Decision Analytics Journal, 6(January), 100163. https://doi.org/10.1016/j.dajour.2023.100163

Alarfaj, F. K., Malik, I., Khan, H. U., Almusallam, N., Ramzan, M., & Ahmed, M. (2022). Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms. IEEE Access, 10(April), 39700–39715. https://doi.org/10.1109/ACCESS.2022.3166891

Alatawi, M. N. (2025). Machine Learning with Applications Detection of fraud in IoT based credit card collected dataset using machine learning. Machine Learning with Applications, 19(May 2024), 100603. https://doi.org/10.1016/j.mlwa.2024.100603

Bansal, A., & Garg, H. (2021). An Efficient Techniques for Fraudulent detection in Credit Card Dataset: A Comprehensive study. IOP Conference Series: Materials Science and Engineering, 1116(1), 012181. https://doi.org/10.1088/1757-899x/1116/1/012181

Bin Sulaiman, R., Schetinin, V., & Sant, P. (2022). Review of Machine Learning Approach on Credit Card Fraud Detection. Human-Centric Intelligent Systems, 2(1–2), 55–68. https://doi.org/10.1007/s44230-022-00004-0

Charizanos, G., Demirhan, H., & İçen, D. (2024). An online fuzzy fraud detection framework for credit card transactions. Expert Systems with Applications, 252(April). https://doi.org/10.1016/j.eswa.2024.124127

de Amorim, L. B. V., Cavalcanti, G. D. C., & Cruz, R. M. O. (2023). The choice of scaling technique matters for classification performance. Applied Soft Computing, 133, 1–37. https://doi.org/10.1016/j.asoc.2022.109924

Dornadula, V. N., & Geetha, S. (2019). Credit Card Fraud Detection using Machine Learning Algorithms. Procedia Computer Science, 165, 631–641. https://doi.org/10.1016/j.procs.2020.01.057

Hussein, A. S., Khairy, R. S., Mohamed Najeeb, S. M., & Salim ALRikabi, H. T. (2021). Credit Card Fraud Detection Using Fuzzy Rough Nearest Neighbor and Sequential Minimal Optimization with Logistic Regression. International Journal of Interactive Mobile Technologies, 15(5), 24–42. https://doi.org/10.3991/ijim.v15i05.17173

Ileberi, E., Sun, Y., & Wang, Z. (2021). Performance Evaluation of Machine Learning Methods for Credit Card Fraud Detection Using SMOTE and AdaBoost. IEEE Access, 9, 165286–165294. https://doi.org/10.1109/ACCESS.2021.3134330

Ileberi, E., Sun, Y., & Wang, Z. (2022). A machine learning based credit card fraud detection using the GA algorithm for feature selection. Journal of Big Data, 9(1). https://doi.org/10.1186/s40537-022-00573-8

Itoo, F., Meenakshi, & Singh, S. (2021). Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection. International Journal of Information Technology (Singapore), 13(4), 1503–1511. https://doi.org/10.1007/s41870-020-00430-y

Kilickaya, O. (2024). Credit Card Fraud Detection: Comparison of Different Machine Learning Techniques. International Journal of Latest Engineering and Management Research (IJLEMR), 9(2), 15–27. https://doi.org/10.56581/ijlemr.9.02.15-27

Knn, R. U., & Regression, L. (2023). Credit Card Fraud Detection : An Improved Strategy for High.

Leevy, J. L., Hancock, J., & Khoshgoftaar, T. M. (2023). Comparative analysis of binary and one-class classification techniques for credit card fraud data. Journal of Big Data, 10(1). https://doi.org/10.1186/s40537-023-00794-5

Madhurya, M. J., Gururaj, H. L., Soundarya, B. C., Vidyashree, K. P., & Rajendra, A. B. (2022). Exploratory analysis of credit card fraud detection using machine learning techniques. Global Transitions Proceedings, 3(1), 31–37. https://doi.org/10.1016/j.gltp.2022.04.006

Razaque, A., Frej, M. B. H., Bektemyssova, G., Amsaad, F., Almiani, M., Alotaibi, A., Jhanjhi, N. Z., Amanzholova, S., & Alshammari, M. (2023). Credit Card-Not-Present Fraud Detection and Prevention Using Big Data Analytics Algorithms. Applied Sciences (Switzerland), 13(1). https://doi.org/10.3390/app13010057

Yan, C., Wang, J., Zou, Y., Weng, Y., Zhao, Y., & Li, Z. (2024). Enhancing Credit Card Fraud Detection Through Adaptive Model Optimization.