JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 6, Desember 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i6.9343
Hal 837-846
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Credit Card Fraud Detection in Bank Using Ensemble Variation: Logistic Regression, Support Vector Classifier and Random Forest

Chlyfen Richard Salibana[1], Ema Utami[2*]

[1] Magister Teknik Informatka, PJJ Informatika, Universitas Amikom Yogyakarta, Yogyakarta, Indonesia
[2] Doktoral Informatika, Universitas Amikom Yogyakarta, Yogyakarta, Indonesia
Email: [1]chlyfenrichard@students.ac.id, [2*]ema.u@amikom.ac.id
Email Penulis Korespondensi: ema.u@amikom.ac.id
Submitted **14-11-2025;** Accepted **06-12-2025;** Published **15-12-2025**

Abstrak

Fraud kartu kredit merupakan ancaman signifikan dalam industri keuangan yang menyebabkan kerugian finansial yang sangat tinggi setiap tahunnya sehingga menjadi tantangan bagi para pelaku usaha maupun sektor keuangan. Hal ini menjadi bagian yang perlu diteliti dan dilakukan pengembangan untuk mengetahui model fraud yang memiliki peningkatan signifikan setiap waktu. Tujuan penelitian ini mengembangkan sistem deteksi fraud kartu kredit berbasis machine learning (ML) dengan pendekatan ensemble, guna mengatasi tantangan data yang tidak seimbang pada transaksi keuangan digital. Metode yang digunakan meliputi empat tahapan utama yaitu: pengumpulan data; SMOTE; Hyper Parameter Tuning; dan evaluasi model. Dataset yang digunakan dari Kaggle Kredit Card Fraud Detection yang memiliki proporsi fraud sangat rendah (0,17%). Peningkatan jumlah data dilakukan dengan SMOTE pada data training. Tiga model utama (Logistic Regression, Support Vector Classifier, Random Forest) serta ensemble (hard dan soft voting) diuji dengan hyperparameter tuning untuk hasil optimal. Random forest memiliki kinerja terbaik dengan F1-Score 0,8482 dan ROC-AUC 0,9684, model ini mampu mendeteksi 84% tranaksi fraud dengan presisi tinggi, melampaui model lain dalam penanganan data imbalance. Keunggulan kombinasi RF dan SMOTE efektif untuk deteksi fraud relevan untuk sistem realtime di sektor keuangan.

Kata Kunci: Credit Card Fraud Detectio; Machine dan Ensemble Learning; Random Forest; SMOTE; Imbalanced Data

Abstract

Credit card fraud is a significant threat in the financial industry, causing significant financial losses annually, posing a challenge to both businesses and the financial sector. This requires research and development to identify fraud models that significantly improve over time. The purpose of this research is to develop a machine learning (ML)-based credit card fraud detection system with an ensemble approach to address the challenges of imbalanced data in digital financial transactions. The method used includes four main stages: data collection; SMOTE; Hyperparameter Tuning; and model evaluation. The dataset used is from Kaggle Credit Card Fraud Detection, which has a very low fraud proportion (0.17%). The increase in data volume was carried out using SMOTE on the training data. Three main models (Logistic Regression, Support Vector Classifier, Random Forest) and ensembles (hard and soft voting) were tested with hyperparameter tuning for optimal results. Random Forest performed best with an F1-Score of 0.8482 and an ROC-AUC of 0.9684. This model was able to detect 84% of fraudulent transactions with high precision, surpassing other models in handling imbalanced data. The combined advantages of RF and SMOTE are effective for fraud detection which is relevant for real-time systems in the financial sector.

Keywords: Credit Card Fraud Detection; Machine and Ensemble Learning; Random Forest; SMOTE; Imbalanced Data

1. PENDAHULUAN

Perkembangan digital dengan era transformasi saat ini yang sangat pesat sehingga menjadikan kartu kredit sebagai alat pembayaran mengalami peningkatan signifikan. Seiring dengan kemajuan ini, kasus *fraud* kartu kredit juga meningkat secara drastis, menyebabkan kerugian finansial besar bagi institusi keuangan dan konsumen. Deteksi *fraud* kartu kredit menjadi tantangan karena karakteristik datanya yang tidak seimbang, di mana jumlah transaksi fraud hanya sebagian kecil dari total populasi data. Metode konvensional berbasis statistik telah terbukti kurang efektif terhadap pola penipuan yang terus berubah. Sehingga pendekatan yang berbasis *machine learning* (ML) semakin banyak digunakan karena kemampuannya dalam mempelajari pola dan menganalisis data dalam jumlah besar secara otomatis [1][2] dalam penelitian yang telah dilakukan ini menghasilkan model deteksi fraud kartu kredit berbasis kombinasi SMOTE-KMEANS dan ensemble deep learning (Bi-LSTM, Bi-GRU, CNN + XGBoost) yang kinerjanya lebih baik dibanding model klasik. Algoritma SMOTE-KMEANS terbukti memberikan peningkatan AUC terbesar pada berbagai classifier dibanding SMOTE biasa, akan tetapi masih memiliki kekurangan penggunaan datset hanya satu dan pendekatan model cukup kompleks (SMOTE-KMEANS + Bi-LSTM + Bi-GRU + CNN + XGBoost, bagging), sehingga implementasi nyata di sistem produksi bisa menuntut sumber daya komputasi tinggi dan pengelolaan model yang rumit.

Salah satu tantangan utama dalam penerapan ML untuk deteksi penipuan adalah mengatasi ketidakseimbangan data. Ketika model yang digunakan berdistribusi dengan kelas yang tidak proporsional, kinerjanya cenderung lebih dominan terhadap transaksi normal dan mengabaikan transaksi bersifat abnormal yang justru lebih penting dalam hal ini transaksi penipuan [3][4]. Untuk mengatasi masalah tersebut, metode *Synthetic Minority Over-sampling Technique* (SMOTE) banyak digunakan sebagai teknik penyeimbangan data yang efektif. SMOTE menghasilkan kelas pada sampel buatan minoritas, sehingga memungkinkan untuk dapat di kaji lebih representative [5][6]. Dalam penelitian ini, algoritma klasifikasi Logistic Regression digunakan sebagai model baseline, yang dikombinasikan dengan SMOTE untuk mendeteksi penipuan secara akurat.

JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 6, Desember 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i6.9343
Hal 837-846
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Masalah utama dalam deteksi penipuan kartu kredit adalah ketidakseimbangan data (*imbalanced data*), di mana jumlah transaksi normal jauh lebih besar dibandingkan dengan transaksi penipuan. Hal ini mengakibatkan model cenderung bias terhadap kelas mayoritas, sehingga mengurangi akurasi dalam mendetksi kasus penipuan yang sebenarnya *crucial*. Pendekatan supervised learning lebih efektif dibandingkan unsupervised apabila data telah diproses untuk mengatasi ketidakseimbangan, pentingnya data balancing dan memperkenalkan strategi kombinasi dengan ensemble learning untuk meningkatkan sensitivitas terhadap kelas minoritas. Masalah lain yang muncul adalah kebutuhan model yang efisien namun tetap akurat untuk digunakan dalam sistem real-time. Model yang terlalu kompleks seringkali sulit diterapkan dalam lingkungan yang membutuhkan waktu prediksi cepat dan interpretabilitas yang tinggi [2].

Berbagai model telah digunakan untuk deteksi penipuan, mulai dari model klasik hingga pendekatan berbasis deep learning. Logistic Regression sering digunakan sebagai baseline karena sifatnya yang sederhana dan dapat dijelaskan, serta memberikan hasil yang cukup baik pada dataset yang telah seimbang. Evaluasi yang dilakukan terhadap beberapa metode seperti *Logistic Regression*, *Decision Tree*, dan *AdaBoost* dengan bantuan teknik SMOTE, menunjukkan bahwa *Logistic Regression* tetap memberikan performa yang kompetitif, terutama dalam hal kecepatan dan interpretabilitas. *Autoencoder Neural Network* untuk mendeteksi anomali dalam dataset *imbalanced*, sedangkan Marco et al. [7] mengusulkan arsitektur *hybrid* CNN-LSTM berbasis *attention mechanism* untuk menangkap hubungan temporal dalam data transaksi. Selain itu, Zhu et al. [3] mengintegrasikan *Neural Network* dengan SMOTE dan membuktikan bahwa kombinasi tersebut mampu secara signifikan meningkatkan akurasi dan recall terhadap kasus penipuan. Sundaravadivel et al. [6] juga membuktikan bahwa Random Forest yang dikombinasikan dengan SMOTE mampu menghasilkan F1 score yang tinggi dan lebih stabil. Hasil dari penelitian tersebut menunjukkan bahwa dengan SMOTE akan membarikan keseimbangan data yang sangat membantu untuk digunakan dalam riset dan pengembangan topik *fraud* kartu kredit.

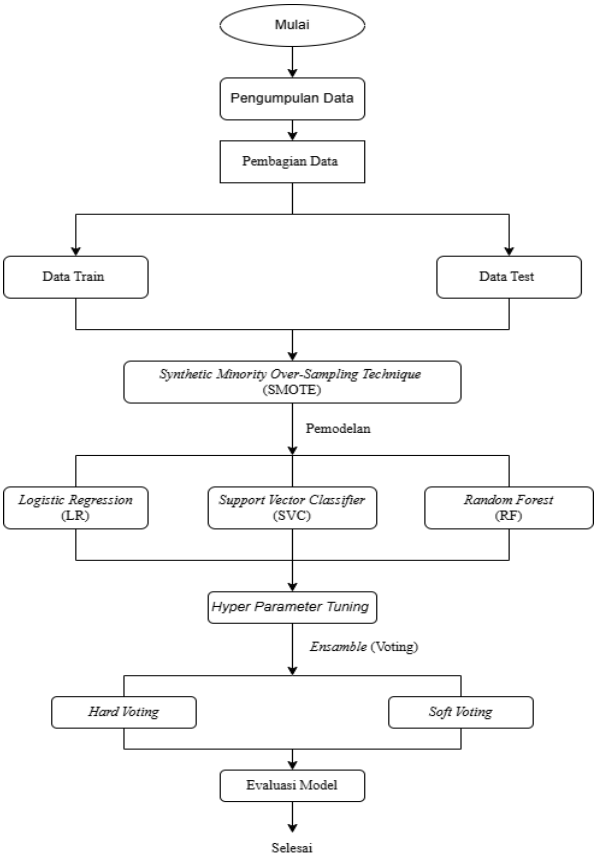
Evaluasi kinerja model lama studi terdahulu umumnya dilakukan menggunakan metrik seperti *Accuracy, Precision, Recall* dan terutama F1-Score, karena metrik ini lebih representatif untuk kondisi data yang tidak seimbang. Gostkowski et al. [8] mencatat bahwa performa deteksi sangat bergantung pada kombinasi algoritma dan teknik balancing. Wang [4] memperkenalkan FS-SMOTE yang secara signifikan meningkatkan recall terhadap kelas fraud. Sementara itu, studi oleh Carcillo et al. [9] menunjukkan bahwa strategi *active learning* juga dapat digunakan dalam deteksi *fraud* berbasis data streaming secara dinamis. Berbagai studi tersebut mengkonfirmasi bahwa performa model akan meningkat secara signifikan apabila digunakan bersama metode penyeimbangan data yang tepat, terutama pada masalah dengan distribusi kelas yang sangat tidak merata.

Berdasarkan latar belakang diatas, dapat disimpukan bahwa: (1). Ketidakseimbangan kelas merupakan tantangan sentral dalam sistem deteksi penipuan; (2). Teknik SMOTE secara konsisten berhasil meningkatkan kemampuan model dalam mengenali kelas minoritas; (3) Logistic Regression tetap relevan sebagai baseline yang ringan namun efektif, terutama bila dikombinasikan dengan teknis balancing seperti SMOTE; dan (4). Studi lebih lanjut mendorong pengguna model hybrid dan teknik ensemble untuk peningkatan lebih lanjut terhadap performa dan ketahanan sistem. Hal ini menjadi dasar untuk menganalisis kembali faktor-faktor fraud yang terjadi pada kredit card dengan menggunakan metode *Logistic Regression, Support Vector Classifier* dan *Random Forest* yang telah di SMOTE terlebih dahulu.

2. METODOLOGI PENELITIAN

Bagian ini menjelaskan tahapan yang dilakukan dalam penelitian seperti yang ditunjukkan pada alur **Gambar 1**. Selanjutnya untuk detail tahapan penelitian serta metode yang digunakan akan dibahas pada masing-masing sub bab.

JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 6, Desember 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i6.9343
Hal 837-846
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom



Gambar 1. Alur Penelitian

2.1 Pengumpulan dan Pembagian Data

Fitur-fitur dalam penelitian ini terdiri dari V1 hingga V28 yang merupakan komponen *principal*, serta dua fitur original yaitu t*ime* (detik sejak transaksi pertama) dan a*mount* (jumlah transaksi). Fitur target Class memiliki nilai 1 untuk fraud dan 0 untuk *legitimate transaction* [10]. Penelitian ini menggunakan dataset *Credit Card Fraud Detection* yang tersedia secara publik di *platform* Kaggle. Dataset ini berisi transaksi kartu kredit yang dilakukan oleh pemegang kartu Eropa selama periode September 2013. Total dataset terdiri dari 284.807 transaksi dengan 492 transaksi fraud (0,17%) dan 284.315 transaksi *legitimate* (99,83%), menjukkan *extreme class imbalance* yang menjadi karakteristik khas *fraud detection problems*. Dataset memiliki 31 fitur numerik hasil transformasi *Principal Component Analysis* (PCA) untuk menjaga *confidentially*. Data training adalah data yang digunakan untuk mengajar model. Data tersebut akan digunakan kemudian untuk monitor performa model ML yang digunakan serta untuk memnghindari hasil yang *overfitting* dan kemudian untuk mengukur akurasi dan prediksi [11].

2.2 Preprocessing Data

Tahap preprocessing dimulai dengan *feature scalling* menggunakan *Standart Scaler* pada fitur Time dan Amount untuk menormalisasi distribusi dan memastikan semua fitur memiiki skala yang *comparable*. *Standar Scaler* mentransformasi fitur dengan mean 0 dan standart deviation 1 menggunakan formula *z*-score untuk normalisasi data berikut yang ditunjukkan pada persamaan (1) [10].

$$z = \frac{x-\mu}{\sigma} \quad (1)$$

Dimana:
x adalah nilai asli
μ adalah nilai rata-rata dari fitur
σ adalah standar deviasi dari fitur

Normalisasi ini *crucial* karena algoritma SVC dan Logistic Regression sensitif terhadap skala fitur. Kemudian data dibagi menjadi *training set* (80%) dan *test* (20%) menggunakan *stratified splitting* untuk mempertahankan proporsi kelas pada kedua subset. *Stratified* sampling memastikan bahwa distribusi *fraud transactions* tetap terjaga pada data training dan data test untuk mendapatkan evaluasi yang fair dan representatif. Sehingga bentuk data dapat diuji dengan model algoritma yang akan digunakan [12]. Pembagian data dilakukan dengan model 80/20, hal ini dipilih karena penggunaan data yang besar. Rasio 80/20 telah terbukti secara empiris menghasilkan akurasi dan performa yang lebih stabil dibandingkan pembagian lain seperti 70/30 atau 60/40 dalam banyak penelitian [13].

JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 6, Desember 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i6.9343
Hal 837-846
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

2.3 Penanganan Imbalanced Data dengan SMOTE

Proses untuk mengatasi ketidakseimbangan kelas pada dataset dengan membuat sampel sintetis untuk kelas minoritas [14]. Keunggulan dari menggunakan SMOTE pada dataset yang tidak seimbang ini adalah, akan meningkatkan jumlah sampel di kelas minoritas (anomaly) sehingga model tidak hanya berfokus pada kelas mayoritas (normal), mengurangi *false negative*, sehingga lebih banyak *anomaly* yang terdeteksi, meningkatkan AUC (*Area Under Curve*) dalam ROC Curve yang menunjukkan model lebih baik dalam membedakan kelas, nilai dari precision, recall, dan f1-score lebih seimbang antara kelas mayoritas dan minoritas sehingga akan mempengaruhi hasil dari akurasi.

Extreme class imbalance (0,17% fraud) menjadi tantangan utama yang harus diatasi karena dapat menyebabkan model bias terhadap kelas mayoritas dan menghasilkan performa yang buruk pada fraud detection. Penelitian ini menerapkan SMOTE untuk menyeimbangkan distribusi kelas pada data training. SMOTE bekerja dengan mensintesis sampel minoritas baru menggunakan interpolasi antara kelas minoritas dan tetangga terdekat-nya. Algoritma SMOTE melakukan Langkah-langkah berikut:

a. untuk setiap sampel minoritas, identifikasi k-nearest neighbors dari kelas yang sama;
b. pilih satu atau lebih tetangga secara random;
c. buat data synthetic baru pada titik random antara sampel original dan tetangga yang dipilih menggunakan formula pada persamaan (2)

$$x_{new} = x\_{i} + \lambda \times (x\_neighbor - x_i) \quad (2)$$

Dimana :
λ *adalah* bilangan random antara 0 dan 1.

Penerapan SMOTE pada data training menghasilkan dataset yang seimbang dengan 228.457 sampel fraud dan 228.457 sampel normal, menjadi total 456.914 sampel. SMOTE hanya diterapkan pada data training untuk menghindari data leakage, sedangkan data uji tetap mempertahankan distribusi original untuk evaluasi yang realistis terhadap kondisi yang ada. Dalam penelitian ini kombinasi SMOTE dengan pembagian data 80/20 merupakan best practice modern dalam machine learning untuk kasus data imbalance, baik pada algoritma klasik (K-Nearest Neighbors, Naive Bayes, Random Forest, SVC, Logistic Regression) maupun model yang lebih kompleks.

SMOTE membantu model machine learning agar tidak hanya "belajar" dari kelas mayoritas, sehingga meningkatkan kemampuan model dalam mengenali dan memprediksi data dari kelas minoritas. Penerapan SMOTE pada training set menghasilkan dataset yang perfectly balanced dengan 228.457 sampel fraud dan 228.457 sampel legitimate, total 456.914 sampel. Perlu dicatat bahwa SMOTE hanya diterapkan pada training set untuk menghindari data leakage, sedangkan test set tetap mempertahankan distribusi original untuk evaluasi yang realistis terhadap real-world performance.

2.4 Pemodelan

Penelitian ini memakai tiga algoritma ML yakni; Logistic Regression, Support Vector Classifier and Random Forest. Pemilihan ketiga algorimta ML ini berdasarkan faktor kompleksitas model, kepopulerannya dalam riset dan efisiensi dalam komputasi dan riset yang berkembang saat ini.

a. Logistic Regression merupakan salah satu teknik pemodelan matematika yang digunakan untuk memperoleh hubungan antara variabel dependen biner dengan satu atau lebih variabel independen. Variabel independen bisa berupa kontinu, diskrit, atau biner, atau bisa berasal dari berbagai kombinasi jenis variabel tersebut [15]. Logistic regression ini mempunyai interpretabilitas tinggi, tetapi kurang efektif dalam menangani data yang tidak terpisahkan secara linear. Dalam metode ini, variabel dependen bersifat biner, yaitu bernilai 1 (Ya) atau 0 (Tidak). Logistic Regression merupakan bentuk regresi linier yang biasa digunakan untuk memetakan sejumlah variabel numerik ke dalam variabel biner atau probabilistik, persamaan untuk Logistic Regression digunakan persamaan 3 berikut:

$$P(y = 1|X) = \frac{1}{1+e^{(\beta_0+\beta_1 x_1+\beta_2 x_1+\cdots+\beta_p x_p)}} \quad (3)$$

Dimana:
$P(y = 1|X)$ adalah probabilitas bahwa kelasnya 1
β adalah koefisien yang dipelajari oleh model
x adalah fitur input

b. Support vector classifier (SVC) merupakan bagian dari algoritma Support Vector Machine (SVM) yang berfokus pada klasifikasi [16]. Algoritma Support Vector Machine (SVM) adalah algoritma yang bertujuan untuk menemukan hyperplane maksimal. Hyperplane merupakan fungsi yang mampu memisahkan dua kelas. SVM memaksimalkan margin atau jarak antara pola pelatihan dan batas keputusan. Terdapat sejumlah keunggulan dari algoritma ini, seperti memiliki performa yang bagus, baik pada data berjumlah kecil maupun besar, serta performa yang optimal pada data yang memiliki banyak atribut. Algoritma ini juga mudah diimplementasikan [17]. SVM dapat digunakan pada klasifikasi linier atau non linier. Metode ini mengajarkan area yang memisahkan antar kategori dalam sebuah observasi. Metode ini efektif untuk data berdimensi tinggi tetapi memiliki kompleksitas komputasi yang tinggi. Rumus untuk perhitungan SVM menggunakan persamaan Kernel RBF untuk pemisahan non-linier, pemilihan ini dikarenakan dapat menangkap pola yang lebih kompleks dan juga lebih cepat serta stabil dalam proses pelatihan

JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 6, Desember 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i6.9343
Hal 837-846
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

karena tidak perlu menghitung pangkat tinggi, Secara keseluruhan, kernel RBF sering menjadi pilihan default karena keseimbangan antara fleksibilitas, kinerja, dan efisiensi komputasi. Untuk rumus dasar pemisahan hyperplane seperti pada persamaan 4 berikut:

$$f(x) = \omega * \phi(x) + b \quad (4)$$

Dimana:

ω adalah vektor bobot (normal vector) dari hyperplane
$\phi(x)$ adalah pemetaan fungsi kernel (RBF) dari data x ke ruang fitur yang lebih tinggi
b adalah bias (intercept)

c. Metode Random Forest memiliki dua fungsi untuk pemecahan suatu kasus, yaitu klasifikasi dan prediksi. Teknik dasar yang digunakan adalah pohon keputusan. Dengan kata lain metode Random Forest merupakan kumpulan pohon keputusan untuk klasifikasi dan prediksi data dengan memberikan masukan ke dalam akar di bagian atas kemudian turun ke daun di bagian bawah. Hasil analisis metode Random Forest untuk klasifikasi adalah bentuk setiap pohon dari pohon-pohon yang terbangun, sedangkan hasil prediksi diperoleh dari nilai rata-rata setiap pohon. Metode Random Forest merupakan hasil pengembangan metode Classification and Regression Tree (CART) yang menerapkan metode agregasi bagging atau bootstrap dan pemilihan fitur secara acak. Algoritma Random Forest mempunyai nilai m yang dapat berbeda-beda. Nilai m merupakan banyaknya variabel prediktor yang digunakan sebagai pemisah dalam pembentukan pohon klasifikasi. Nilai m yang semakin besar akan menyebabkan korelasi yang semakin tinggi [18]. Random Forest memberikan hasil yang kompetitif dibandingkan dengan algoritma lain, namun tidak mengubah data secara progresif. Berikut pada persamaan 5 yang digunakan dalam random forest.

$$Gini(D) = 1 - (p_1^2 + p_2^1) \quad (5)$$

Dimana:
P adalah probabilitas dari kelas 1 dan kelas 2 dalam dataset D

2.5 Hyperparameter Tuning

Proses untuk mendapatkan kombinasi parameter terbaik terhadap setiap model, maka harus dilakukan proses hyperparameter tuning menggunakan optimasi GridSearchCV [19].

2.6 Evaluasi Model

Setelah tahap pemodelan dengan tiga algoritma yang berbeda, peneliti melanjutkan ke tahap evaluasi untuk menilai kinerja masing-masing model dalam mendeteksi credit card yang mengalami fraud. Kinerja dari setiap model akan divisualisasikan dalam bentuk grafik dan tabel, selanjutnya akan dicari nilai akurasi, presisi, dan recall, serta f1-score serta perbandingan model dan performa akan divisualisasikan dalam bentuk kurva ROC sehingga nantinya bisa mendapatkan model yang terbaik dalam mendeteksi intrusi jaringan.

3. HASIL DAN PEMBAHASAN

3.1 Hasil

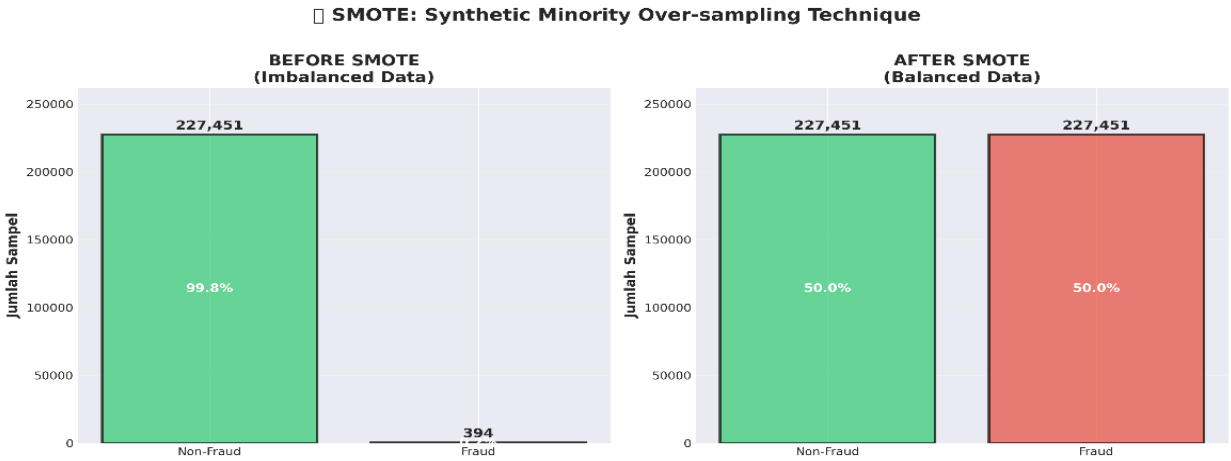
3.1.1 Pengumpulan dan Persiapan Data

Pengumpulan data dilakukan dengan akses data pada *platform* Kaggle yang telah menyediakan data dari berbagi sumber untuk dijadikan bahan penelitian. Akses yang lebih mudah dan transparan menjadi nilai tambah sebagai data penelitian yang akan digunakan. Sedangkan untuk persiapan data, total dataset terdiri dari 284.807 transaksi dengan 492 transaksi fraud (0,17%) dan 284.315 transaksi *legitimate* (99,83%), menjukkan *extreme class imbalance* yang menjadi karakteristik khas *fraud detection problems*. Data tersebut kemudian dibagi dengan *split data* menjadi data train dan data test.

3.1.2 Preprocessing Data

Penggunaan data perlu dilakukan proses seleksi sekaligus tahap awal terlebih dahulu dan mengubah data mentah menjadi format yang lebih baik serta sesuai untuk analisis maupun pelatihan model ML. Tahap ini juga merupakan tahap yang *crucial* sebelum dilakukan analisis data karena dalam tahapan inilah yang akan menentukan kualitas dari data yang digunakan untuk menghasilkan hasil data uji yang akurat. Hal ini menjadi bagian yang penting karena akan menjadi penentu kualitas data yang digunakan dan kesiapan data untuk dianalisis yang akan menghasilkan prediksi model ML lebih akurat [20]. Berdasarkan hasil pengujian yang dilakukan dalam tahapan ini, didapatkan hasil seperti pada **Gambar 2** berikut.

JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 6, Desember 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i6.9343
Hal 837-846
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

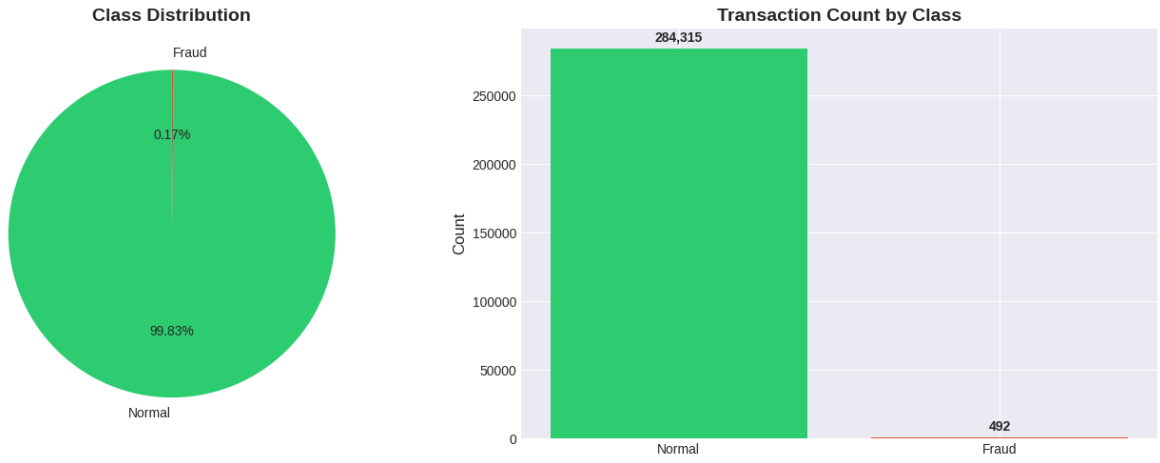


Gambar 2. Persentase distribusi transaksi yang mengalami *fraud* dan non-*fraud*

Hasil pengujian dalam penelitian ini menunjukkan bahwa total dataset terdiri dari 284.807 dimana transaksi fraud sebanyak 492 (0.17%) dan transaksi *no fraud* sebanyak 284.315 (99,83%) , menunjukkan *extreme imbalance* yang menjadi karakteristik khas pada *fraud detection*. Dataset memiliki 31 fitur numerik hasil transformasi *Principal Component Analysis* (PCA) untuk menjaga kerahasiaan data. Fitur-fitur tersebut terdiri dari V1 hingga V28 yang merupakan komponen principal, serta dua fitur original yaitu Time dan *Amount* (jumlah_transaksi). Fitur kelas target memiliki nilai 1 untuk fraud dan 0 untuk transaksi sah.

3.1.3 Penanganan Imbalanced Data dengan SMOTE

Ketidakseimbangan data ekstrim data fraud (0,17%) menjadi tantangan utama yang harus diatasi karena dapat menyebabkan model bias terhadap kelas no fraud dan dapat menghasilkan performance yang buruk pada *fraud detection system.* Penelitian ini menerapkan *Synthetic Minority Over-sampling Technique* (SMOTE) untuk menyeimbangkan distribusi kelas [21]. Penerapan SMOTE pada training set menghasilkan dataset yang seimbang dengan 228.457 sampel *fraud* dan 228.457 sampel *no fraud* total data menjadi 456.914 sampel. Setelah pembagian data selesai, pemodelan akan dilakukan menggunakan lima algoritma machine learning (ML), yaitu Logistic Regression (LR), Random Forest (RF), Support Vector Classifier (SVC), Hard Voting (HV) dan Soft Voting (SV). Untuk mendapatkan hasil yang diinginkan, pemodelan ini akan dilakukan dengan menggunakan *Hyperparameter Tuning* dan tanpa *Hyperparameter Tuning*. Hasil SMOTE ditunjukkan pada **Gambar 3** berikut.



Gambar 3. Hasil pengujian SMOTE

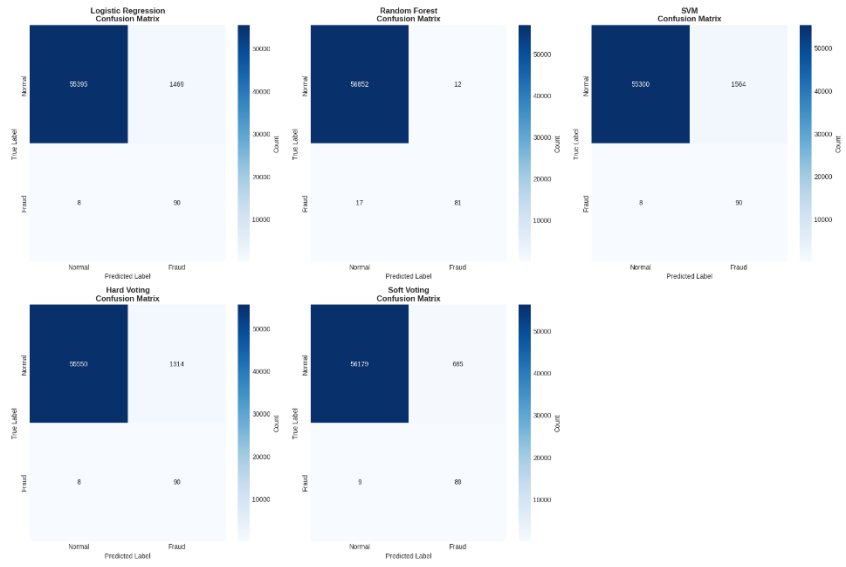
Parameter SMOTE yang digunakan yaitu k_neighbors=5 berarti bahwa untuk setiap sampel kelas minoritas, SMOTE akan mencari 5 tetangga terdekat (nearest neighbors) dari kelas minoritas tersebut, lalu membuat data sintetis baru dengan interpolasi antara sampel tersebut dan salah satu tetangganya secara acak. Dengan nilai ini, variasi data sintetis yang dihasilkan akan cukup, tetapi tidak terlalu banyak sehingga menghindari noise berlebihan. Dengan Parameter sampling_strategy=1.0 menunjukkan bahwa SMOTE akan membuat jumlah sampel sintetis pada kelas minoritas hingga jumlahnya sama dengan kelas mayoritas, sehingga rasio kelas minoritas dan mayoritas menjadi 1:1. Ini berarti semua kelas minoritas akan di-oversample hingga seimbang dengan kelas mayoritas.

JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 6, Desember 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i6.9343
Hal 837-846
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Penerapan SMOTE hanya pada data training bertujuan untuk meningkatkan kinerja model saat pelatihan, bukan untuk memanipulasi data pengujian (test data). Jika SMOTE diterapkan pada seluruh dataset sebelum pembagian, maka data sintetis akan bocor ke data test, menyebabkan evaluasi model menjadi tidak valid karena data test tidak lagi mewakili kondisi dunia nyata. Oleh karena itu, SMOTE harus dilakukan setelah data dibagi, hanya pada data training agar hasil evaluasi tetap objektif dan tidak terjadi data *leakage*

3.1.4 Pemodelan Data

Pemodelan dalam penelitian ini digunakan 5 jenis model algoritmik ML, yaitu; Logistic reggession, support vector classifier, random forest, hard voting, dan hard voting. Pemodelan ini merujuk pada konseptual, logis dan fisik. Tujuan utama dari pemodelan ini adalah untuk mengorganisasi dan menstrukturkan data mentah ke dalam format yang sesuai agar model *machine learning* dapat belajar, mengidentifikasi pola, dan menghasilkan prediksi yang akurat [22]. Pada Tabel 1 berikut merupakan hasil pengujian dari masing-masing model algoritmik ML yang digunakan dalam pemodelan data penelitian ini. Dengan Gambar 4 untuk confusion matrix hasil dari pengujian dalam penelitian ini.



Gambar 4. Confusion Matrix

Tabel 1. Nilai Confusion Matrix Hasil Penelitian

No	Algoritma ML	F1-Score	Akurasi	Presisi	Recall	ROC-AUC
1	Logistic Regression	0,1086	0,9741	0,0577	0,9184	0,9708
2	Support Vector Classifier	0,1027	0,9724	0,0544	0,9184	0,9750
3	Random Forest	0,8482	0,9995	0,8710	0,8265	0,9684
4	Hard Voting	0,1198	0,9768	0,0641	0,9184	-
5	Soft Voting	0,2041	0,9878	0,1150	0,9082	0,9737

Berdasarkan hasil pengujian seperti yang ditunjukkan pada Tabel 1 diatas, algoritma ML untuk LR, SVC, Hard Voting dan Soft Voting menunjukkan bahwa nilai *f1*-score yang berarti bahwa model klasifikasi ini memiliki kinerja yang kurang baik untuk data fraud yang digunakan. Hal ini juga menunjukkan bahwa model tersebut memiliki masalah serius baik dalam *presisi* (banyak memprediksi positif palsu) atau *recall* (banyak melewatkan kasus positif yang sebenarnya). Bahkan ketidakseimbangan data ini karena nilai yang sangat rendah, sehingga sering kali muncul pada dataset yang tidak seimbang (*imbalanced dataset*), di mana model mungkin jarang memprediksi kelas minoritas dengan benar. Sedangkan nilai yang paling baik ditunjukkan oleh RF dengan nilai *f1*-score sebesar 0,8410, ini menunjukkan bahwa algoritma yang memiliki kinerja paling baik dengan keseimbang antara *presisi* dan *recall* yang baik pula. Nilai 0,84 ini berarti model RF mampu mengidentifikasi sebagian besar kasus positif dengan benar (*recall* yang baik) dan, pada saat yang sama, tidak sering salah mengklasifikasikan kasus negatif sebagai positif (*presisi* yang baik).

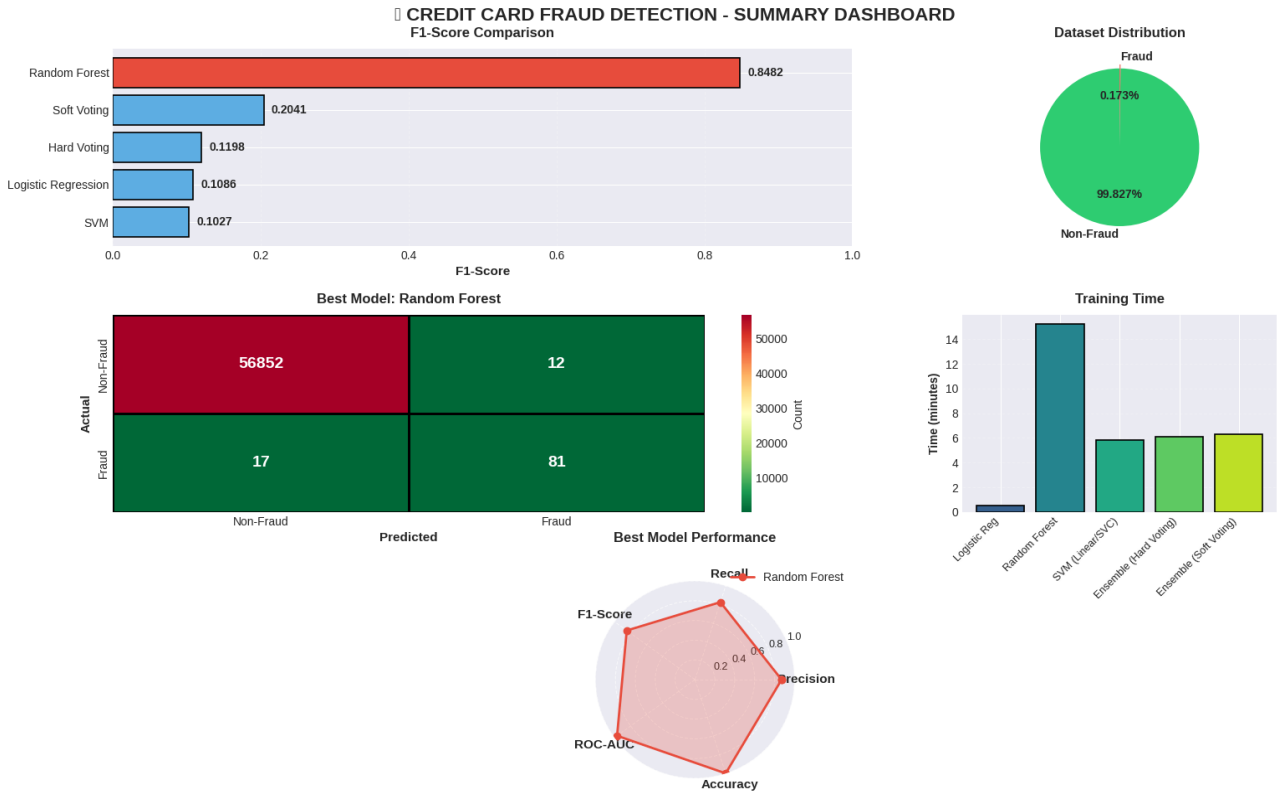
Model LR dan SVC memiliki akurasi sangat tinggi, namun F1-Score, Presisi sangat rendah dan Recall sangat tinggi. Ini menandakan model hanya sedikit memprediksi kelas minoritas namun hampir selalu benar saat memprediksi kelas tersebut. Hal ini tipikal pada data imbalance jika model tidak menangani kelas minoritas dengan baik. Akurasi tinggi karena banyak sekali prediksi benar pada kelas mayoritas. Sedangkan untuk model RF menunjukkan keseimbangan di seluruh metrik, dengan F1-Score, Presisi, dan Recall yang tinggi. Ini berabrti bahwa RF mampu mengenali kelas minoritas sekaligus tidak mengorbankan presisi, sehingga penyeimbangannya baik dan hasil lebih reliabel terutama untuk data tidak

JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 6, Desember 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i6.9343
Hal 837-846
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

seimbang. Untuk model Voting (Hard dan Soft) menunjukkan performa lebih baik dari LR dan SVC, tetapi belum mampu menyaingi RF dalam nilai F1-Score dan Presisi. Nilai ROC-AUC pada seluruh model selain Hard Voting umumnya tinggi (>0,96), menandakan model cukup baik dalam membedakan dua kelas secara probabilistik, tetapi hal ini tidak otomatis berarti baik pada prediksi kelas minoritas secara nyata, karena masih harus mempertimbangkan komponen nilai yang lain dalam cakupannya.

3.2 Pembahasan

Nilai dari pemodelan selanjutnya dilakukan *Hyper parameter tuning* untuk evaluasi dari pengujian yang telah dilakukan. Sehingga didapatkan hasil seperti yang ditunjukkan pada **Gambar 5** dan **6** berikut ini. Berdasarkan **Gambar 5**, menunjukkan bahwa dalam pengujian ini menghasilkan bahwa algoritma ML RF adalah yang memiliki kinerja paling baik diantara yang lain. Hal ini juga menunjukkan bahwa pemodelan dengan RF dapat memiliki nilai akurasi dan presisi yang baik dalam keseimbangannya. Dengan penggunaan data dalam jumlah yang besar, RF masih dapat digunakan untuk pengujian dalam penelitian pengembangan analisis fraud di sektor perbankan. RF unggul dibandingkan SVC dan LR terutama pada data yang kompleks dan imbalance karena karakteristik dua aspek utama yaitu kemampuan membuat *non-linear decision boundary* dan *robustness* dari teknik *bagging* yang digunakan. RF terdiri dari banyak *decision tree* yang mampu membentuk *decision boundary* yang sangat fleksibel dan tidak linear, sehingga dapat menyesuaikan kompleksitas distribusi data dengan jauh lebih baik daripada LR yang terbatas hanya pada *boundary linear*. SVC memang mampu menghasilkan *non-linear boundary* dengan kernel tertentu (seperti RBF), tapi tetap rentan terhadap *noise* dan tidak memiliki mekanisme *ensemble* yang menurunkan variansi model. Sehingga, RF lebih efektif menangkap pola yang rumit dan interaksi antar fitur, sehingga lebih baik dalam mengklasifikasi kelas minoritas pada data imbalance.

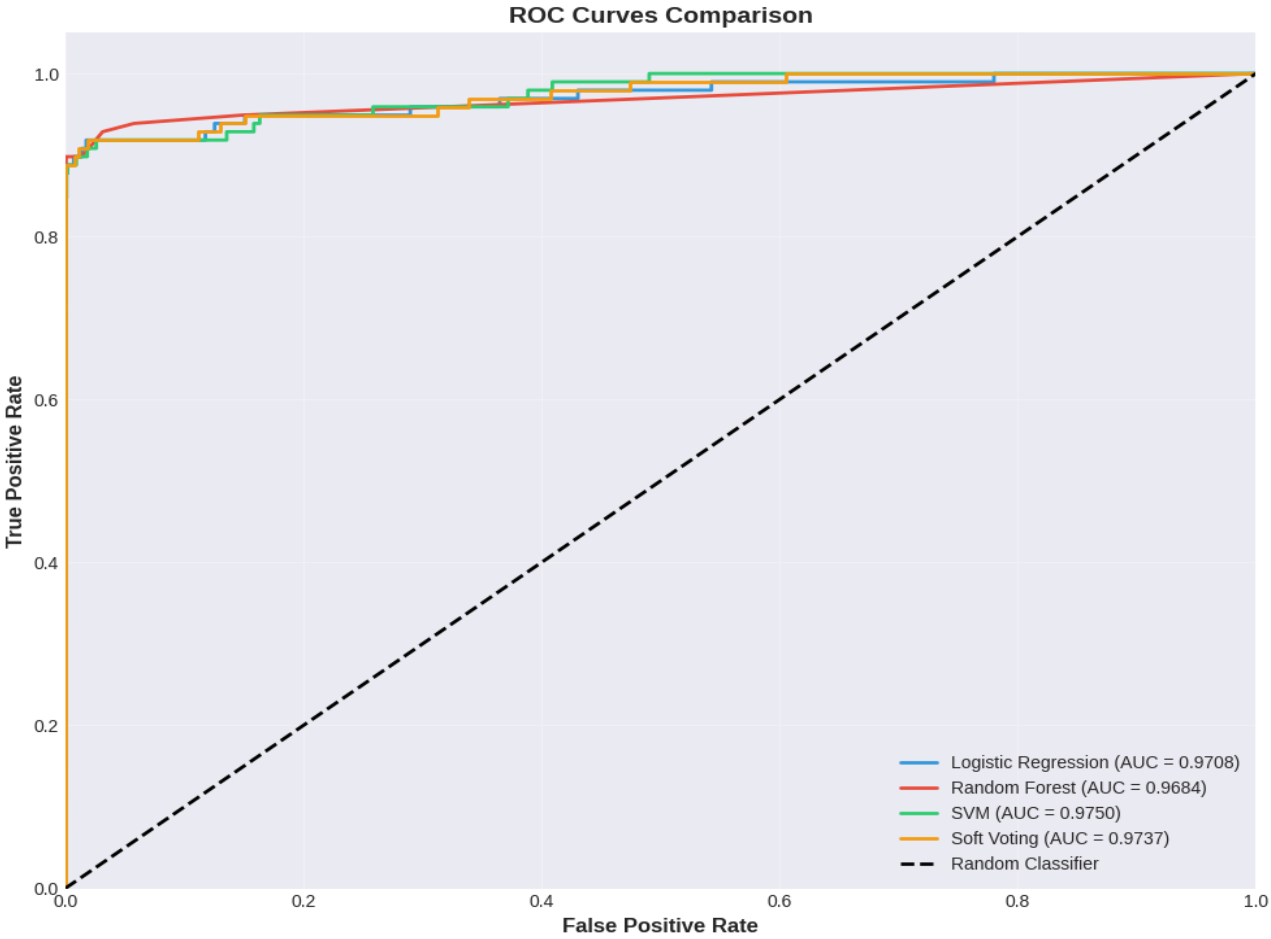


Gambar 5. Hasil pengujian penelitian secara keseluruhan

RF menggunakan prinsip *bagging* (*bootstrap aggregating*), yaitu dengan membangun banyak pohon keputusan dari data dan fitur yang diacak. Hasil dari banyak pohon ini nantinya rata-rata (*voting*) sehingga prediksi menjadi lebih stabil dengna keuntungan utama *bagging* adalah turunnya variasi model tanpa meningkatkan bias secara signifikan. SVC dan LR tidak menerapkan *bagging*, sehingga lebih sensitif terhadap *noise*, outlier, dan kurang *robust* jika distribusi data berubah-ubah. Selain itu, RF cukup tahan terhadap *overfitting* karena akumulasi banyak model sederhana yang masing-masing hanya "melihat" sebagian data dan fitur. RF adaptif pada data yang tidak linear dan besar, akan tetapi SVC/LR terbatas jika *boundary* data sangat rumit, sedangkan RF dapat membentuk banyak *boundary* dari hasil voting pohon. Dengan kombinasi *bagging* dan *random feature selection* membuat RF kokoh terhadap *overfitting* dan variasi, yang merupakan dua masalah utama pada *data imbalance* dan *real world,* RF juga dilengkapi kemampuan mengukur pentingnya fitur (*feature importance*) dan menangani data *high dimension* tanpa "*collapse*" *accuracy*.

JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 6, Desember 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i6.9343
Hal 837-846
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Hasil ini konsisten dan sama dengan studi sebelumnya [2] dan [6] yang mengembangkan system untuk deteksi *Credit Card Fraud* yang berbasis ML, khususnya untuk mengatasi masalah data yang sangat *imbalance* (proporsi fraud < 0,2%). Model utama yang diuji adalah RF, dengan teknik oversampling SMOTE untuk menyeimbangkan kelas minoritas. Hasil dari penelitian tersebut menunjukkan bahwa RF sebagai model terbaik, dengan akurasi 99,5%, precision dan recall tinggi (~0,98). Model ini mampu mengenali transaksi fraud tanpa terlalu banyak kesalahan positif (false positive) maupun negatif (false negative). Dengan penerapan SMOTE sangat *crucial* agar model dapat mengidentifikasi pola fraud, karena tanpa teknik ini model cenderung bias ke kelas mayoritas (transaksi sah). Sistem ini dapat langsung diintegrasikan ke infrastruktur pemrosesan transaksi secara real-time, mengurangi kerugian finansial dan meningkatkan kepercayaan konsumen. Web interface yang dibuat juga friendly dan dapat digunakan non-teknisi.



Gambar 6. Kurva ROC

Berdasarkan **Gambar 6** diatas, menunjukkan bahwa untuk kelima model yang diuji. Secara keseluruhan, semua model menunjukkan performa yang sangat baik dengan nilai AUC (Area Under Curve) berkisar antara 0,9684 hingga 0,9750, yang mengindikasikan kemampuan diskriminasi yang excellent dalam membedakan transaksi normal dan fraud. Support Vector Machine dengan Linear SVC kernel mencapai nilai AUC tertinggi sebesar 0,9750, diikuti oleh LR dan Ensemble Soft Voting dengan nilai AUC 0,9737. Meskipun perbedaan nilai AUC antar model relatif kecil, hal ini menunjukkan bahwa pemilihan algoritma yang tepat dan *hyperparameter tuning* yang optimal telah berhasil memaksimalkan performa deteksi fraud.

Karakteristik kurva ROC yang menunjukkan kenaikan tajam (steep rise) pada bagian awal kurva mengindikasikan bahwa model-model tersebut mampu mencapai True Positive Rate (TPR) yang tinggi dengan False Positive Rate (FPR) yang masih rendah. Kondisi ini sangat ideal dalam konteks deteksi fraud, karena sistem dapat mengidentifikasi sebagian besar transaksi fraud dengan meminimalkan false alarm yang dapat mengganggu pengalaman pengguna legitimate.Performa yang hampir serupa antar model (ditunjukkan dengan kurva ROC yang saling overlap) dapat dijelaskan oleh beberapa faktor: Pertama, penggunaan SMOTE telah berhasil mengatasi masalah *class imbalance* dengan menyeimbangkan distribusi data training. Hal ini memungkinkan setiap algoritma untuk belajar dengan baik dari kedua kelas tanpa bias terhadap kelas mayoritas. Kedua, preprocessing yang komprehensif termasuk standardisasi fitur telah memfasilitasi proses pembelajaran yang optimal. Fitur-fitur yang telah melewati transformasi PCA memiliki karakteristik yang memungkinkan berbagai algoritma untuk ekstrak pola dengan efektif. Ketiga, hyperparameter tuning menggunakan

JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 6, Desember 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i6.9343
Hal 837-846
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

GridSearchCV dengan cross-validation telah mengoptimalkan setiap model untuk mencapai performa maksimal pada dataset ini. Hal ini menunjukkan bahwa dengan tuning yang tepat, berbagai algoritma dapat mencapai performa yang kompetitif. Meskipun demikian, terdapat perbedaan penting dalam interpretabilitas dan kompleksitas komputasi antar model. RF, meskipun memiliki AUC yang sedikit lebih rendah dibanding SVM, menawarkan keunggulan dalam hal interpretabilitas melalui *feature importance* dan *computational efficiency* yang lebih baik untuk *deployment* dalam *production environment*.

Ensemble methods (*Soft Voting*) menunjukkan performa yang konsisten dengan AUC 0.9737, memvalidasi pendekatan ensemble learning dalam meningkatkan robustness prediksi. Soft Voting yang menggunakan rata-rata probabilitas dari base classifiers memberikan hasil yang identik dengan RF, mengindikasikan bahwa RF memiliki kontribusi dominan dalam ensemble tersebut.Perbandingan dengan Random Classifier (AUC = 0,5000) yang ditunjukkan oleh garis diagonal putus-putus menegaskan bahwa semua model yang dikembangkan memiliki kemampuan prediktif yang signifikan. Jarak vertikal yang besar antara kurva model dengan diagonal *random classifier* mengindikasikan discriminative power yang kuat dalam membedakan kelas. Dari perspektif praktis, model dengan AUC > 0,97 dianggap excellent dan siap untuk implementasi dalam sistem deteksi fraud real-time. Performa yang tinggi ini mengindikasikan bahwa sistem dapat mendeteksi hampir seluruh transaksi fraud (high sensitivity) sambil menjaga tingkat false alarm yang rendah (*high specificity*).

Potensi penerapan model RF-SMOTE pada sistem real-time fraud monitoring dan integrasi ke sistem keuangan sangat menjanjikan untuk diintegrasikan pada sistem fraud detection real-time di dunia finansial. Dengan teknologi API, model bisa "menyaring" transaksi mencurigakan secara real-time dan scalable, memberikan proteksi proaktif pada transaksi konsumen dan lembaga keuangan. Hal ini karena kelebihan model RF-SMOTE memiliki deteksi kuat untuk Data Tidak Seimbang: Random Forest yang dilatih dengan data hasil balancing SMOTE mampu mendeteksi transaksi fraud walaupun proporsinya sangat kecil (misal <0,2%). Studi empiris terbaru menunjukkan model ini memiliki akurasi 97–99,5% dan F1-score serta recall sangat tinggi, sehingga jarang melewatkan kasus fraud, ahan terhadap outlier, noise, dan tetap stabil saat memasukkan data baru, yang sangat penting untuk transaksi keuangan real-time. Sehingga model dapat dimasukkan ke API scoring engine. Prosesnya: tiap transaksi masuk, fitur diekstrak dan distandarisasi, lalu model memprediksi skor fraud (atau langsung prediksi 0/1). Sehingga prediksi bisa dilakukan dalam hitungan milidetik—sesuai untuk sistem real-time (contohnya pada layanan transaksi online atau sistem alert bank)

4. KESIMPULAN

Berdasarkan hasil dan pembahasan, dapat disimpulkan bahwa nilai F1-Score menunjukkan yang paling baik adalah model algoritmik RF yakni 84% dari total data yang menjadi bahan penelitian sedangkan kurva roc menunjukkan hal yang signifikan dengan nilai 96. Performa RF dapat diatribusikan pada kemampuan ensemble internal-nya dalam menangkap *complex non-linear patterns* dan interaksi *features* dalam *fraud detection context*. Penelitian ini memberikan kontribusi praktis bagi lembaga keuangan dalam memilih dan menerapkan sistem deteksi penipuan yang efektif, menunjukkan bahwa model RF-SMOTE yang digunakan dapat mencapai kinerja luar biasa dalam mendeteksi transaksi *credit card fraud* dengan data set yang tidak seimbang. Potensi penerapan model RF-SMOTE pada sistem real-time fraud monitoring dan integrasi ke sistem keuangan sangat menjanjikan untuk diintegrasikan pada sistem fraud detection real-time di dunia finansial.

REFERENCES

[1] Y. Wang, “A Data Balancing and Ensemble Learning Approach for Credit Card Fraud Detection,” *2025 4th Int. Symp. Comput. Appl. Inf. Technol. ISCAIT 2025*, pp. 386–390, 2025, doi: 10.1109/ISCAIT64916.2025.11010591.
[2] E. Ileberi, Y. Sun, and Z. Wang, “Performance Evaluation of Machine Learning Methods for Credit Card Fraud Detection Using SMOTE and AdaBoost,” *IEEE Access*, vol. 9, pp. 165286–165294, 2021, doi: 10.1109/ACCESS.2021.3134330.
[3] J. Z. Jiang Ping, Jinliang Zhang, “Credit Card Fraud Detection Using Autoencoder Neural Network,” *Cornell Univ.*, vol. 2, no. 1, pp. 35–41, 2019, doi: 10.1016/j.gltp.2021.01.006.
[4] Y. Wang, “Fraud detection based on FS-SMOTE model for credit card,” *Highlights Sci. Eng. Technol.*, vol. 70, pp. 316–323, 2023, doi: 10.54097/hset.v70i.12479.
[5] M. Zhu, Y. Zhang, Y. Gong, C. Xu, and Y. Xiang, “Enhancing Credit Card Fraud Detection: A Neural Network and SMOTE Integrated Approach,” *J. Theory Pract. Eng. Sci.*, vol. 4, no. 02, pp. 23–30, 2024, doi: 10.53469/jtpes.2024.04(02).04.
[6] P. Sundaravadivel, R. A. Isaac, D. Elangovan, D. KrishnaRaj, V. V. L. Rahul, and R. Raja, “Optimizing credit card fraud detection with random forests and SMOTE,” *Sci. Rep.*, vol. 15, no. 1, 2025, doi: 10.1038/s41598-025-00873-y.
[7] R. Marco, N. Aini, and I. M. A. Agastya, “A Hybrid Approach CNN-LSTM Based on Attention Mechanism for Credit Card Fraud Detection,” *Int. J. Intell. Eng. Syst.*, vol. 18, no. 3, pp. 653–664, 2025, doi: 10.22266/ijies2025.0430.45.
[8] A. N. Gostkowski Michał, Andrzej Krasnodębski, “Credit Card Fraud Detection Using Machine Learning Techniques,” *Lect. Notes Networks Syst.*, vol. XXVII, no. 2, pp. 571–585, 2024, doi: 10.1007/978-981-97-2004-0_21.
[9] F. Carcillo, Y. A. Le Borgne, O. Caelen, and G. Bontempi, “Streaming active learning strategies for real-life credit card fraud detection: assessment and visualization,” *Int. J. Data Sci. Anal.*, vol. 5, no. 4, pp. 285–300, 2018, doi: 10.1007/s41060-018-0116-z.
[10] M. Arif and A. D. Hartono, “Jurnal Informatika : Jurnal pengembangan IT Menggunakan Metode Machine Learning Untuk

Memprediksi Nilai Mahasiswa Dengan Model Prediksi Multiclass," vol. 10, no. 1, pp. 190–204, 2025, doi: 10.30591/jpit.v9ix.xxx.

[11] I. Carolina and T. Haryanto, "JITE (Journal of Informatics and Telecommunication Engineering) Modeling Of Hyperparameter Tuned RNN-LSTM and Deep Learning," vol. 7, no. January, pp. 502–513, 2024.

[12] I. Akbar, F. Supriadi, and D. Indra Junaedi, "Pemanfaatan Machine Learning Di Bidang Kesehatan," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 9, no. 1, pp. 1744–1749, 2025, doi: 10.36040/jati.v9i1.12663.

[13] R. Nurhidayat and K. E. Dewi, "KOMPUTA : Jurnal Ilmiah Komputer dan Informatika PENERAPAN ALGORITMA K-NEAREST NEIGHBOR DAN FITUR EKSTRAKSI N-GRAM DALAM ANALISIS SENTIMEN BERBASIS ASPEK," *Komputa J. Ilm. Komput. dan Inform.*, vol. 12, no. 1, pp. 91–100, 2023, [Online]. Available: https://www.kaggle.com/datasets/hafidahmusthaanah/skincare-review?select=00.+Review.csv.

[14] F. D. Astuti and F. N. Lenti, "Implementasi SMOTE untuk mengatasi Imbalance Class pada Klasifikasi Car Evolution menggunakan K-NN," *J. JUPITER*, vol. 13, no. 1, pp. 89–98, 2021.

[15] E. Purwanto, "Prediksi Performa Mahasiswa Menggunakan Model Regresi Logistik," vol. 9, no. 2, pp. 145–152, 2022.

[16] M. Furqan, R. Kurniawan, and K. I. Hp, "Evaluasi Performa Support Vector Machine Classifier Terhadap Penyakit Mental," vol. 02, pp. 203–210, 2020, doi: 10.21456/vol10iss2pp203-210.

[17] N. Rochmawati, A. K. Zyen, N. A. Widiastuti, and T. N. I. Bill, "Comparison of Support Vector Machine (SVM) and Random Forest Algorithms in the Analysis of Social Media X User Sentiment Towards the TNI Bill," vol. 9, no. 5, pp. 2854–2860, 2025.

[18] S. Mahmuda and U. Mulawarman, "Implementasi Metode Random Forest pada Kategori Konten Kanal Youtube," vol. 2, no. 01, pp. 21–31, 2024.

[19] M. Iqbal, H. M. Nawawi, M. R. R. Saelan, M. S. Maulana, Yudhistira, and A. Mustopa, "PREDIKSI DAYA BELI MOBIL," *J. Manaj. Inform. Sist. Inf.*, vol. 6, no. 1, pp. 73–81, 2023.

[20] T. Gori *et al.*, "PREPROCESSING DATA DAN KLASIFIKASI UNTUK PREDIKSI KINERJA DATA PREPROCESSING AND CLASSIFICATION FOR PREDICTING STUDENT," vol. 11, no. 1, pp. 215–224, 2024, doi: 10.25126/jtiik.20241118074.

[21] S. A. Putri and R. Rachmatika, "Penerapan Algoritma Random Forest dan SMOTE untuk Prediksi Risiko Putus Sekolah Siswa Sekolah Menengah Kejuruan," vol. 5, no. 3, pp. 903–910, 2025.

[22] M. A. T. Ramadhani *et al.*, "Pemodelan Prediksi Nilai IQ Menggunakan Algoritma Machine Learning," *J. Teknol. Dan Sist. Inf. Bisnis*, vol. 7, no. 2, pp. 262–267, 2025, doi: 10.47233/jteksis.v7i2.1851.