Peningkatan Kinerja Deteksi Penipuan Digital dengan Teknik SMOTE dan Komparasi Algoritma Klasifikasi

Improving Digital Fraud Detection Performance Using SMOTE and Comparative Analysis of Classification Algorithms

[1]Niko Akbar*, [2] Yandi Anzhari, [3]Oki Dahwanu, [4]Nurul Abdillah
[1,2,3,4]Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Jambi
[1,2,3,4]Jl. Jambi-Muara Bulian KM. 15, Mendalo Indah, Kecamatan Jambi Luar Kota, Kabupaten Muaro Jambi, Jambi.
*e-mail: nikoakbar@unja.ac.id

(***received*:** 30 July 2026, ***revised*:** 3 October 2026, ***accepted*:** 21 October 2026)

Abstrak

Transformasi digital pada platform media sosial X (sebelumnya Twitter) memicu peningkatan kasus penipuan digital (fraud). Pendekatan machine learning umum digunakan untuk mendeteksi penipuan, namun menghadapi tantangan ketidakseimbangan kelas (class imbalance), di mana cuitan penipuan jauh lebih sedikit dibandingkan cuitan normal. Penelitian ini bertujuan mengevaluasi pengaruh teknik Synthetic Minority Over-sampling Technique (SMOTE) terhadap kinerja deteksi penipuan, serta membandingkan tiga algoritma klasifikasi: *Naive Bayes*, *Support Vector Machine* (SVM), dan *Logistic Regression*. Data bersumber dari dataset Kaggle "ScamTags: Indonesian NER for Fraud Identification" dengan ekstraksi fitur TF-IDF. Untuk mencegah *Data Leakage*, pemisahan data latih dan uji dilakukan secara ketat di dalam proses Cross Validation, sehingga SMOTE hanya diterapkan pada lipatan (fold) data latih dan tidak pernah menyentuh data uji. Hasil eksperimen menunjukkan bahwa pada dataset berukuran kecil dan tidak seimbang ini, penerapan SMOTE tidak secara konsisten meningkatkan kinerja. *Naive Bayes* merupakan satu-satunya model yang mampu mendeteksi penipuan secara efektif, dengan recall tertinggi sebesar 90,00% dan F-Measure 60,76% pada skenario tanpa SMOTE. Sebaliknya, SVM gagal mendeteksi kelas penipuan (recall 0%) meskipun akurasinya tampak tinggi. Temuan ini menegaskan pentingnya evaluasi bebas *Data Leakage* dan menyoroti bahwa metrik akurasi dapat menyesatkan pada data tidak seimbang, sehingga recall dan F-Measure kelas minoritas lebih representatif untuk menilai sistem deteksi penipuan. Secara praktis, penelitian ini memberikan rujukan bahwa model sederhana seperti *Naive Bayes* dapat menjadi pilihan awal yang andal untuk penyaringan cuitan penipuan berbahasa Indonesia, khususnya ketika data pelatihan masih terbatas. Meskipun demikian, hasil penelitian perlu dimaknai dengan mempertimbangkan keterbatasan ukuran dataset yang kecil dan berasal dari satu sumber, sehingga generalisasi temuan memerlukan validasi pada data yang lebih besar dan beragam.

Kata kunci: *data leakage, fraud detection, imbalanced data, naive bayes, SMOTE, twitter.*

Abstract

The digital transformation of social media platforms, particularly X (formerly Twitter), has been accompanied by an increase in digital fraud cases. Machine learning approaches are widely used for fraud detection; however, they face the challenge of class imbalance, in which fraudulent posts are substantially outnumbered by legitimate posts. This study aims to evaluate the effect of the Synthetic Minority Over-sampling Technique (SMOTE) on fraud detection performance and compare three classification algorithms: Naive Bayes, Support Vector Machine (SVM), and Logistic Regression. The data were obtained from the Kaggle dataset "ScamTags: Indonesian NER for Fraud Identification," with features extracted using Term Frequency–Inverse Document Frequency (TF-IDF). To prevent data leakage, training and test data were strictly separated within the cross-validation procedure, ensuring that SMOTE was applied exclusively to the training folds and never to the test data. The experimental results show that, for this small and imbalanced dataset, SMOTE did not consistently improve model performance. Naive Bayes was the only model that effectively detected fraudulent posts, achieving the highest recall of 90.00% and an F-measure of 60.76% in the scenario without

 ISSN:2302-8149
e-ISSN:2540-9719

SMOTE. In contrast, SVM failed to detect the fraud class, yielding a recall of 0%, despite its seemingly high accuracy. These findings underscore the importance of leakage-free evaluation and highlight how accuracy can be misleading when dealing with imbalanced data. Consequently, minority-class recall and F-measure provide more informative measures for evaluating fraud detection systems. In practical terms, this study suggests that a simple model such as Naive Bayes can serve as a reliable initial option for screening Indonesian-language fraudulent posts, particularly when training data are limited. Nevertheless, these findings should be interpreted in light of the dataset's small size and single-source origin. Further validation using larger and more diverse datasets is required to establish the generalizability of the results.
Keywords: *data leakage, fraud detection, imbalanced data, naive bayes, SMOTE, twitter.*

1 Pendahuluan

Transformasi ke arah digitalisasi telah memicu lonjakan kasus penipuan (*fraud*) di berbagai platform, termasuk media sosial X (sebelumnya Twitter). Penipuan seperti *phishing*, pencurian identitas, dan manipulasi informasi digital menimbulkan kerugian finansial yang signifikan serta merusak kepercayaan pengguna [1], [2], [3], [4], [5]. Mengandalkan sistem deteksi konvensional berbasis aturan (*rule-based*) dinilai tidak lagi memadai karena sulit beradaptasi dengan pola kejahatan yang terus berkembang [1], [2], [6].

X merupakan salah satu alat komunikasi yang digunakan untuk menyebarkan informasi kepada banyak orang tanpa terbatas ruang dan waktu [7]. Platform ini juga berfungsi sebagai jejaring sosial dan *mikroblogging* daring yang memungkinkan pengguna mengirim dan membaca pesan berbasis teks dengan batasan 280 karakter, yang disebut kicauan atau *tweet* [7], [8], [9]. Selain memberikan dampak positif, media sosial juga membuka peluang kejahatan, termasuk pelaksanaan modus penipuan di dunia maya.

Mendeteksi cuitan penipuan secara manual hampir tidak mungkin dilakukan mengingat volume dan persebarannya yang sangat luas, sehingga diperlukan pendekatan *machine learning*. Namun, pendekatan ini menghadapi tantangan utama berupa ketidakseimbangan kelas (*class imbalance*), di mana jumlah cuitan penipuan (kelas minoritas) jauh lebih sedikit dibandingkan cuitan normal (kelas mayoritas) [2], [10], [11], [12], [13]. Kondisi ini menyebabkan algoritma cenderung bias terhadap kelas mayoritas, sehingga model dapat memperoleh akurasi yang tinggi namun memiliki nilai *recall* yang rendah pada kelas penipuan, yang menandakan banyak penipuan lolos dari deteksi [2], [10]. Dalam konteks deteksi penipuan, kegagalan mengenali kasus penipuan jauh lebih merugikan dibandingkan kekeliruan menandai cuitan normal. Oleh sebab itu, evaluasi model tidak cukup bertumpu pada akurasi, melainkan perlu menekankan *recall* dan F-Measure pada kelas minoritas.

Untuk mengatasi bias tersebut, teknik *Synthetic Minority Over-sampling Technique* (SMOTE) banyak digunakan untuk menyeimbangkan distribusi kelas dengan menghasilkan sampel sintetis dari kelas minoritas melalui interpolasi linear antara sampel yang ada dan tetangga terdekatnya [1], [3], [12], [13], [14]. Berbeda dengan *random oversampling* yang hanya menduplikasi data, pendekatan sintesis ini membuat model lebih peka terhadap pola kelas minoritas tanpa sekadar mengulang sampel yang sama. Sejumlah penelitian melaporkan bahwa penerapan SMOTE mampu meningkatkan nilai *recall* pada deteksi penipuan transaksi keuangan. Pengembangan lanjutan seperti SMOTE-ENN dan SMOTE-Tomek juga diusulkan untuk mengurangi *noise* dan tumpang tindih antarkelas. Meskipun demikian, efektivitas SMOTE tetap bergantung pada karakteristik data, termasuk ukuran data dan dimensi fitur yang digunakan.

Berbagai studi juga membandingkan algoritma klasifikasi untuk menentukan model terbaik dalam mendeteksi anomali, mulai dari model dasar seperti *Naive Bayes* dan *Logistic Regression*, model *margin* seperti *Support Vector Machine* (SVM), hingga metode *ensemble* seperti *Random Forest* dan XGBoost [1], [2], [4], [5], [10], [12], [15], [16]. *Naive Bayes* dan *Logistic Regression* umumnya digunakan sebagai model pembanding karena sederhana dan efisien secara komputasi. *Support Vector Machine* dikenal andal pada ruang fitur berdimensi tinggi, namun cenderung memihak kelas mayoritas ketika data sangat tidak seimbang. Sementara itu, metode *ensemble* seperti *Random Forest* dan XGBoost sering melaporkan kinerja tertinggi pada data transaksi numerik yang kompleks. Perbandingan tersebut menunjukkan bahwa tidak ada satu algoritma yang selalu unggul, karena kinerjanya sangat dipengaruhi oleh jenis dan kondisi data.

 ISSN:2302-8149
e-ISSN:2540-9719

Meskipun demikian, sebagian besar penelitian terdahulu masih memiliki keterbatasan yang belum terjawab. Pertama, mayoritas studi menggunakan data transaksi keuangan berbentuk numerik terstruktur[3], [4] , sedangkan deteksi penipuan berbasis teks pada media sosial berbahasa Indonesia masih jarang dieksplorasi. Kedua, banyak studi melaporkan nilai akurasi atau ROC-AUC yang tinggi, namun jarang memeriksa secara eksplisit risiko *Data Leakage* ketika SMOTE diterapkan sebelum pemisahan data, sehingga hasil yang dilaporkan berpotensi terlalu optimis. Ketiga, efektivitas SMOTE pada representasi teks berdimensi tinggi (TF-IDF) dengan ukuran data terbatas belum banyak diuji secara kritis. Penelitian ini berupaya mengisi ketiga celah tersebut dengan mengevaluasi SMOTE pada data teks berbahasa Indonesia melalui prosedur yang bebas dari kebocoran data serta menekankan metrik *recall* dan *F-Measure* pada kelas minoritas.

Berdasarkan uraian tersebut, penelitian ini berfokus pada tiga rumusan masalah, yaitu: (1) bagaimana pengaruh ketidakseimbangan kelas terhadap performa metrik evaluasi, khususnya recall dan F-Measure, dalam deteksi penipuan di X; (2) sejauh mana penerapan teknik *oversampling* SMOTE mampu meningkatkan kemampuan model dalam mengenali kelas minoritas (penipuan); dan (3) algoritma klasifikasi manakah di antara *Naive Bayes*, *Support Vector Machine*, dan *Logistic Regression* yang memberikan kinerja paling optimal dalam mendeteksi penipuan.

Kesenjangan (*gap*): banyak penelitian sebelumnya belum mendemonstrasikan evaluasi yang ketat terhadap *Data Leakage* saat menggunakan SMOTE. Penerapan SMOTE pada keseluruhan data sebelum pemisahan data latih dan data uji berisiko memasukkan sampel sintetis ke dalam data uji, sehingga menghasilkan estimasi kinerja yang terlalu optimistis. Penelitian ini mengisi celah tersebut dengan menempatkan SMOTE hanya pada lipatan data latih di dalam proses *Cross Validation*, sehingga data uji tetap berupa data asli dan evaluasi terbebas dari kebocoran data. Dengan pendekatan ini, perbandingan antara skenario tanpa dan dengan SMOTE dapat dilakukan secara adil. Hasil yang diperoleh pun lebih mencerminkan kemampuan model yang sesungguhnya ketika diterapkan pada data baru.

Penelitian ini bertujuan untuk mengevaluasi pengaruh SMOTE terhadap kinerja deteksi penipuan serta membandingkan ketiga algoritma klasifikasi dalam kondisi evaluasi yang bebas dari *Data Leakage*Secara teoretis, penelitian ini memberikan kontribusi pada literatur *Natural Language Processing* (NLP) dan *machine learning*, khususnya mengenai perilaku algoritma klasifikasi ketika dihadapkan pada sampel sintetis SMOTE pada data teks berdimensi tinggi. Penelitian ini juga menegaskan pentingnya prosedur evaluasi yang bebas dari kebocoran data agar kinerja model tidak dilaporkan secara berlebihan. Secara praktis, hasil penelitian ini dapat menjadi rujukan metodologis dalam membangun model deteksi penipuan berbasis teks. Rujukan tersebut dapat dimanfaatkan oleh pengelola platform media sosial, analis keamanan siber, maupun masyarakat umum untuk memfilter informasi dan memitigasi kerugian finansial akibat penipuan digital.

2 Tinjauan Literatur

2.1 Deteksi Penipuan Digital (*Fraud Detection*)

Penipuan (fraud) secara umum didefinisikan sebagai tindakan tidak jujur yang dilakukan untuk memperoleh keuntungan finansial dari individu atau entitas lain melalui manipulasi atau penyajian fakta palsu yang disengaja. Berbeda dengan pencurian yang melibatkan tindakan sembunyi-sembunyi atau paksaan, penipuan justru meyakinkan korban agar secara sukarela menyerahkan uang atau harta benda [1]. Dalam konteks digital, penipuan dilakukan di dunia maya dan media sosial seperti X (sebelumnya Twitter), Facebook, dan Instagram, dengan modus seperti phishing, pencurian identitas, dan manipulasi informasi yang menimbulkan kerugian finansial signifikan serta merusak kepercayaan pengguna [1], [2], [3].

Karakteristik penipuan di media sosial umumnya bersifat terencana dan mengikuti pola tertentu, sehingga dapat dikenali melalui jejak teks yang ditinggalkan pelaku, seperti ajakan, modus, dan aksi yang berulang. Mengandalkan sistem deteksi konvensional berbasis aturan (*rule-based*) dinilai tidak lagi memadai karena sulit beradaptasi dengan pola kejahatan yang terus berkembang [1], [2], [6]. Oleh karena itu, pendekatan berbasis machine learning banyak digunakan untuk mendeteksi penipuan secara otomatis dan dalam skala besar.

 ISSN:2302-8149
e-ISSN:2540-9719

2.2 Ketidakseimbangan Data (Imbalanced Data)

Ketidakseimbangan kelas (class imbalance) merupakan kondisi di mana jumlah data pada satu kelas jauh lebih sedikit dibandingkan kelas lainnya. Pada kasus deteksi penipuan, proporsi kasus penipuan (kelas minoritas) biasanya jauh lebih kecil dibandingkan transaksi atau aktivitas normal (kelas mayoritas) [1], [12]. Kondisi ini menjadi masalah serius pada machine learning konvensional karena algoritma cenderung bias terhadap kelas mayoritas dan mengabaikan pola kelas minoritas [2], [10], [12], [13].

Akibatnya, model dapat memperoleh nilai akurasi yang tinggi namun gagal mendeteksi kasus penipuan yang sebenarnya, yang ditandai dengan rendahnya nilai recall pada kelas minoritas [2], [10]. Dengan demikian, akurasi bukan merupakan metrik yang representatif pada data tidak seimbang, sehingga diperlukan metrik berbasis kelas minoritas seperti recall dan F-Measure untuk menilai kinerja deteksi secara akurat.

2.3 SMOTE (Synthetic Minority Over-sampling Technique)

SMOTE merupakan teknik penyeimbangan data yang bekerja dengan menghasilkan sampel sintetis dari kelas minoritas, bukan sekadar menduplikasi data yang ada. SMOTE mensintesis data baru melalui interpolasi linear antara suatu sampel minoritas dengan tetangga terdekatnya (k-Nearest Neighbors) [1], [3], [12], [13], [14]. Secara konseptual, untuk setiap sampel minoritas dipilih salah satu tetangga terdekatnya, kemudian dibentuk titik data baru pada garis lurus yang menghubungkan keduanya, sehingga distribusi kelas minoritas menjadi lebih padat dan seimbang terhadap kelas mayoritas.

Beberapa pengembangan menggabungkan SMOTE dengan teknik pembersihan data seperti SMOTE-ENN atau SMOTE-Tomek untuk mengurangi noise dan tumpang tindih antar-kelas [10], [13]. Meskipun demikian, efektivitas SMOTE bergantung pada karakteristik data. Pada dataset berukuran kecil atau berdimensi tinggi, sampel sintetis yang dihasilkan tidak selalu merepresentasikan pola kelas minoritas dengan tepat, sehingga manfaatnya dapat terbatas. Selain itu, penerapan SMOTE harus dilakukan secara hati-hati: SMOTE hanya boleh diterapkan pada data latih dan tidak boleh menyentuh data uji, agar tidak terjadi *Data Leakage* yang menghasilkan estimasi kinerja yang terlalu optimistis.

2.4 Ekstraksi Fitur Teks (TF-IDF)

Untuk dapat diproses oleh algoritma klasifikasi, data teks perlu diubah menjadi representasi numerik melalui proses ekstraksi fitur. Salah satu metode yang banyak digunakan adalah *Term Frequency–Inverse Document Frequency* (TF-IDF). Metode ini memberikan bobot pada setiap kata berdasarkan dua komponen, yaitu *Term Frequency* (TF) yang mengukur frekuensi kemunculan kata dalam sebuah dokumen, dan *Inverse Document Frequency* (IDF) yang mengukur seberapa jarang kata tersebut muncul di seluruh dokumen.

Dengan pembobotan ini, kata yang sering muncul pada satu dokumen tetapi jarang muncul pada dokumen lain akan memperoleh bobot tinggi, karena dianggap lebih informatif dalam membedakan dokumen. Sebaliknya, kata umum yang muncul di hampir seluruh dokumen memperoleh bobot rendah. Representasi TF-IDF menghasilkan vektor berdimensi tinggi yang menjadi masukan bagi algoritma klasifikasi.

2.5 Algoritma Klasifikasi

Penelitian ini membandingkan tiga algoritma klasifikasi yang umum digunakan dalam deteksi anomali dan penipuan, yaitu *Naive Bayes*, *Support Vector Machine*, dan *Logistic Regression*.

Naive Bayes merupakan algoritma klasifikasi probabilistik yang didasarkan pada Teorema Bayes dengan asumsi independensi antar-fitur. Algoritma ini sering digunakan dalam pemrosesan teks karena kesederhanaan dan kecepatan komputasinya, serta efektif pada data berdimensi tinggi seperti hasil TF-IDF [1], [2], [10], [12].

***Support Vector Machine* (SVM)** bekerja dengan mencari hyperplane optimal yang memisahkan dua kelas dengan margin terbesar. SVM dikenal andal pada data berdimensi tinggi, namun kinerjanya pada data yang sangat tidak seimbang dapat menurun karena cenderung memihak kelas mayoritas [11], [12].

 ISSN:2302-8149
e-ISSN:2540-9719

Logistic Regression merupakan model klasifikasi linear yang memperkirakan probabilitas suatu data termasuk dalam kelas tertentu. Algoritma ini sering digunakan sebagai model dasar (baseline) karena kesederhanaannya, meskipun kinerjanya cenderung menurun pada dataset dengan hubungan non-linear yang kompleks [1], [2], [5], [10], [12].

2.6 Metrik Evaluasi Berbasis Confusion Matrix

Kinerja model klasifikasi dievaluasi menggunakan *confusion matrix*, yaitu matriks yang membandingkan hasil prediksi model dengan nilai sebenarnya. Matriks ini terdiri atas empat komponen, yaitu *True Positive* (TP), *True Negative* (TN), *False Positive* (FP), dan *False Negative* (FN). Dalam penelitian ini, kelas penipuan ditetapkan sebagai kelas positif.

Dari keempat komponen tersebut diturunkan tiga metrik utama. Presisi (*Precision*) mengukur proporsi prediksi penipuan yang benar-benar penipuan, dihitung sebagai TP / (TP + FP). Recall mengukur proporsi penipuan yang berhasil terdeteksi dari seluruh penipuan yang sebenarnya, dihitung sebagai TP / (TP + FN). F-Measure merupakan rata-rata harmonik dari presisi dan recall, dihitung sebagai 2 × (Presisi × Recall) / (Presisi + Recall), yang memberikan ukuran kinerja seimbang antara keduanya. Pada konteks deteksi penipuan dengan data tidak seimbang, recall dan F-Measure pada kelas penipuan menjadi tolok ukur yang lebih representatif dibandingkan akurasi.

Pemilihan ketiga algoritma dalam penelitian ini didasarkan pada karakteristik data teks yang bersifat langka dan berdimensi tinggi akibat representasi TF-IDF. *Naive Bayes* dipilih karena efisien dan secara empiris tangguh pada data teks dengan banyak fitur bernilai nol, sehingga sering menjadi acuan pada klasifikasi teks. *Support Vector Machine* dipilih sebagai representasi model *margin* yang secara teoretis unggul pada ruang fitur berdimensi tinggi, meskipun kinerjanya sangat bergantung pada kecukupan jumlah sampel di sekitar batas keputusan. *Logistic Regression* digunakan sebagai model dasar linear untuk pembanding. Dengan demikian, ketiga algoritma mewakili tiga pendekatan berbeda (probabilistik, margin, dan linear) yang memungkinkan analisis mengenai bagaimana karakteristik data teks yang kecil dan tidak seimbang memengaruhi perilaku masing-masing model. Perbedaan pendekatan ini menjadi dasar untuk memahami mengapa model tertentu dapat gagal mengenali kelas minoritas ketika jumlah sampel sangat terbatas.

3 Metode Penelitian

3.1 Pendekatan Penelitian

Penelitian ini menggunakan pendekatan kuantitatif eksperimental untuk membandingkan kinerja tiga algoritma klasifikasi dalam mendeteksi penipuan digital pada platform X, dengan dan tanpa penerapan teknik penyeimbangan data Synthetic Minority Over-sampling Technique (SMOTE). Seluruh tahapan eksperimen, mulai dari pengolahan data hingga evaluasi model, diimplementasikan menggunakan perangkat lunak Altair AI Studio. Tahapan penelitian secara umum terdiri atas pengumpulan data, pembersihan dan pelabelan data, ekstraksi fitur, pelatihan dan pengujian model melalui Cross Validation, serta evaluasi kinerja berbasis confusion matrix.

3.2 Jenis dan Sumber Data

Data yang digunakan dalam penelitian ini bersumber dari dataset publik Kaggle berjudul “ScamTags: Indonesian NER for Fraud Identification”. Dataset asli berbentuk anotasi *Named Entity Recognition* (NER) pada tingkat token, di mana teks dipecah menjadi kata per kata dan setiap kata memiliki tag seperti B-Modus, B-Action, dan O. Karena penelitian ini berfokus pada klasifikasi penipuan pada tingkat cuitan (tweet), data token-level tersebut direkonstruksi kembali menjadi satuan cuitan utuh, kemudian diberi label biner, yaitu penipuan (true) dan bukan penipuan (false).

Cuitan yang mengandung indikasi modus atau aksi penipuan dilabeli sebagai penipuan, sedangkan cuitan yang tidak mengandung indikasi tersebut dilabeli sebagai bukan penipuan. Setelah proses rekonstruksi dan pelabelan, diperoleh dataset akhir yang digunakan dalam eksperimen. Komposisi dataset bersifat tidak seimbang, dengan jumlah cuitan bukan penipuan lebih banyak dibandingkan cuitan penipuan, sehingga merepresentasikan kondisi class imbalance yang menjadi fokus penelitian.

 ISSN:2302-8149
e-ISSN:2540-9719

3.3 Teknik Pengolahan dan Pelabelan Data

Sebelum digunakan, data melalui tahap pembersihan (basic cleaning) untuk menghilangkan data kosong dan duplikat. Cuitan dengan nilai kosong dibuang menggunakan penyaringan data agar tidak mengganggu proses pelatihan dan penyeimbangan data. Selanjutnya, kolom label dikonversi menjadi tipe binominal dan ditetapkan perannya sebagai label kelas. Kelas penipuan (true) ditetapkan sebagai kelas positif, sehingga seluruh metrik evaluasi dihitung berdasarkan kemampuan model mendeteksi penipuan.

3.4 Ekstraksi Fitur

Teks cuitan diubah menjadi representasi numerik melalui proses *Process Documents* dengan pembobotan TF-IDF (*Term Frequency–Inverse Document Frequency*). Tahapan ini mengubah setiap cuitan menjadi vektor bobot kata, di mana kata yang informatif dalam membedakan cuitan memperoleh bobot lebih tinggi. Hasil ekstraksi fitur ini menjadi masukan bagi algoritma klasifikasi.

Perlu menjadi catatan bahwa pada penelitian ini pembentukan kosakata dan pembobotan TF-IDF dilakukan pada keseluruhan Koleksi teks sebelum proses *Cross Validation*. Berbeda dengan SMOTE yang bersifat *supervised* dan sensitif terhadap label, TF-IDF merupakan proses *unsupervised* yang hanya menghitung statistik frekuensi kata tanpa menggunakan informasi label kelas. Oleh karena itu, risiko kebocoran informasi dari tahap ini tergolong minimal dan jauh lebih kecil dibandingkan kebocoran akibat SMOTE. Meskipun demikian, potensi kebocoran terbatas pada tahap pembentukan kosakata tetap diakui sebagai keterbatasan metodologis dan menjadi agenda perbaikan pada penelitian lanjutan, yaitu dengan menempatkan ekstraksi fitur di dalam subproses pelatihan *Cross Validation*.

3.5 Skenario Eksperimen

Penelitian ini menguji dua skenario untuk menilai pengaruh SMOTE terhadap kinerja deteksi penipuan, yaitu:

1. **Skenario tanpa SMOTE** — model dilatih langsung pada data tidak seimbang tanpa penyeimbangan kelas.
2. **Skenario dengan SMOTE** — data latih diseimbangkan menggunakan SMOTE sebelum model dilatih.

Pada kedua skenario, tiga algoritma klasifikasi dibandingkan, yaitu *Naive Bayes*, *Support Vector Machine* (SVM), dan *Logistic Regression*. Dengan demikian, terdapat enam konfigurasi model yang dievaluasi dan dibandingkan kinerjanya.

3.6 Validasi Model dan Pencegahan *Data Leakage*

Untuk memperoleh estimasi kinerja yang valid, model dievaluasi menggunakan Cross Validation. Aspek paling krusial dalam penelitian ini adalah pencegahan kebocoran data (*Data Leakage*) yang dapat terjadi apabila SMOTE diterapkan pada keseluruhan data sebelum pemisahan data latih dan data uji. Apabila hal ini terjadi, sampel sintetis hasil SMOTE dapat masuk ke dalam data uji, sehingga model seolah-olah mengenali data yang mirip dengan data latih dan menghasilkan estimasi kinerja yang terlalu optimistis.

Untuk mencegah hal tersebut, SMOTE tidak diterapkan pada keseluruhan data, melainkan ditempatkan di dalam subproses pelatihan (training) pada operator Cross Validation. Dengan konfigurasi ini, pada setiap iterasi (fold), penyeimbangan data hanya dilakukan pada lipatan data latih, sedangkan lipatan data uji tetap berupa data asli yang tidak pernah disentuh oleh SMOTE. Urutan operator pada subproses pelatihan adalah penyeimbangan data dengan SMOTE, kemudian dilanjutkan dengan pelatihan algoritma klasifikasi. Sementara itu, subproses pengujian terdiri atas penerapan model (Apply Model) pada data uji asli dan perhitungan kinerja (Performance). Dengan demikian, hasil evaluasi yang diperoleh terbebas dari *Data Leakage* dan merepresentasikan kemampuan model yang sesungguhnya.

3.7 Metrik Evaluasi

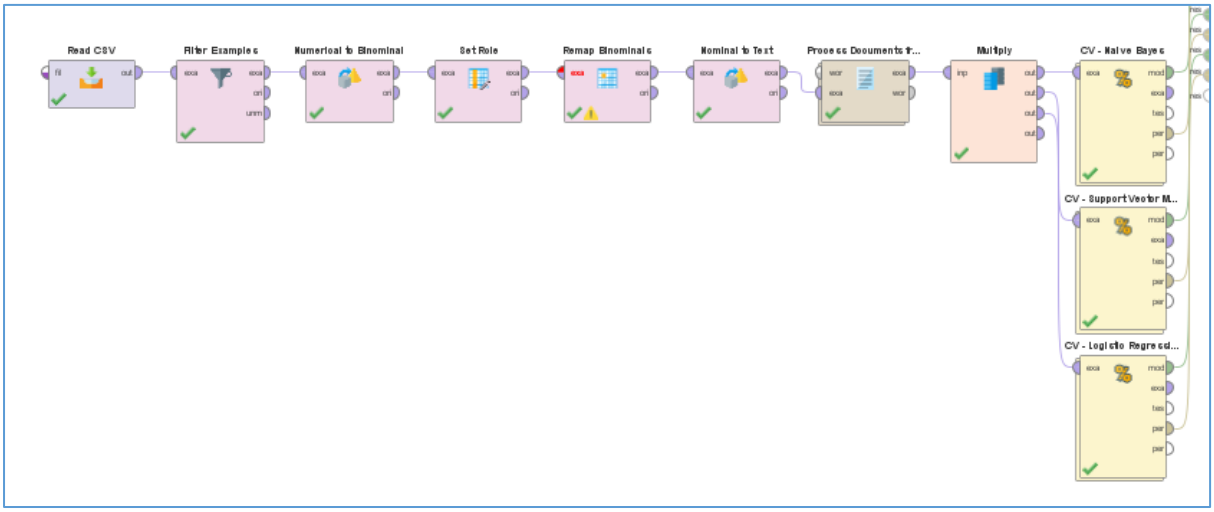
Kinerja setiap model dievaluasi menggunakan confusion matrix dengan kelas penipuan sebagai kelas positif. Metrik yang digunakan meliputi akurasi, presisi (*precision*), *recall*, dan *F-Measure*. Mengingat dataset bersifat tidak seimbang, *recall* dan *F-Measure* pada kelas penipuan menjadi tolok

 ISSN:2302-8149
e-ISSN:2540-9719

ukur utama, sedangkan akurasi diperlakukan sebagai metrik pendukung yang perlu diinterpretasikan secara hati-hati. Presisi dihitung sebagai TP / (TP + FP), recall sebagai TP / (TP + FN), dan F-Measure sebagai rata-rata harmonik dari presisi dan recall.

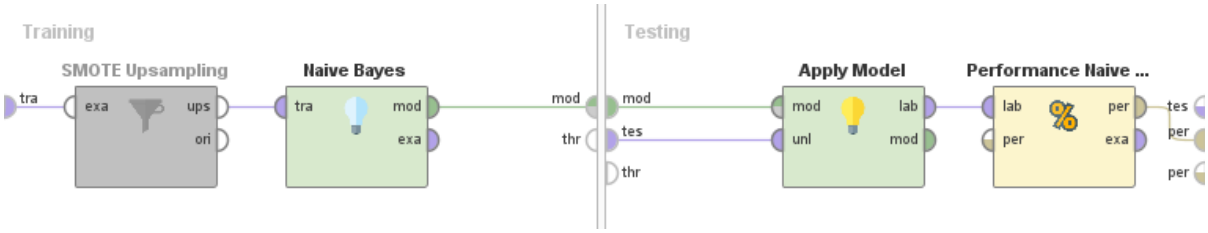
3.8 Tahapan Penelitian

Tahapan penelitian diawali dengan membaca dataset cuitan menggunakan operator Read CSV, kemudian dilanjutkan dengan penyaringan data kosong serta pembersihan data melalui operator Filter Examples. Selanjutnya, kolom label dikonversi menjadi tipe binominal dan ditetapkan perannya sebagai label kelas menggunakan operator Numerical to Binominal dan Set Role, lalu kelas penipuan ditetapkan sebagai kelas positif melalui operator Remap Binominals. Setelah data siap, teks cuitan diubah menjadi vektor fitur berbobot TF-IDF menggunakan operator Nominal to Text dan Process Documents. Vektor fitur tersebut kemudian digunakan untuk melatih dan menguji model melalui Cross Validation, dengan SMOTE ditempatkan di dalam subproses pelatihan pada skenario dengan SMOTE. Tahap terakhir adalah mengevaluasi kinerja model menggunakan confusion matrix serta metrik akurasi, presisi, recall, dan F-Measure. Alur proses penelitian secara keseluruhan ditunjukkan pada Gambar 1.



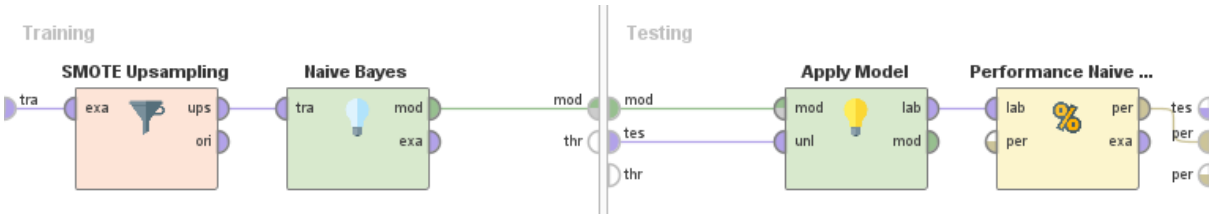
Gambar 1 Skenario proses

Struktur proses Cross Validation untuk skenario tanpa SMOTE ditunjukkan pada Gambar 2, sedangkan struktur untuk skenario dengan SMOTE ditunjukkan pada Gambar 3. Pada skenario dengan SMOTE, operator penyeimbangan data ditempatkan di dalam subproses pelatihan sehingga hanya memengaruhi data latih. Pada skenario dengan SMOTE, operator penyeimbangan data ditempatkan di dalam subproses pelatihan sehingga hanya memengaruhi data latih. Pada skenario tanpa SMOTE, data latih langsung digunakan untuk melatih algoritma klasifikasi, sedangkan subproses pengujian menerapkan model pada data uji asli. Perbedaan kedua struktur tersebut hanya terletak pada keberadaan operator SMOTE, sehingga perubahan kinerja yang terjadi dapat diatribusikan pada penerapan teknik penyeimbangan data.



Gambar 2 Struktur cross validation tanpa SMOTE

 ISSN:2302-8149
e-ISSN:2540-9719



Gambar 3 Struktur cross validation dengan SMOTE

4 Hasil dan Pembahasan

Data mentah hasil rekonstruksi cuitan sebelum proses pembersihan ditunjukkan pada Gambar 4. Untuk mengubah data mentah tersebut menjadi dataset klasifikasi penipuan, dilakukan proses pembersihan dasar (*Basic Cleaning*) dan pelabelan biner pada setiap cuitan. Cuitan yang mengandung indikasi modus atau aksi penipuan diberi label *true*, sedangkan cuitan lainnya diberi label *false*. Data yang bernilai kosong dibuang agar tidak mengganggu proses pelatihan dan penyeimbangan data.

	tweet	label
3	sebetulnya bukannya nggak mau usaha tapi banyak penipuan mindset udah bener tapi kalo misalnya tools nya ternyata menuju scam gimana ketipu terus donk	1
4	sebelumnya gw juga pernah hampir ketipu via interview palsu di linkedin pernah gw tulis di blog ini dan sekarang kejadian mirip keulang lagi bedanya kali ini gw udah diblok duluan chat penawarannya ilang jir keburu diblok duluan	1
5	penting hati hati scam di linkedin gw mau cerita pengalaman nyaris ketipu sama proyek web3 palsu via linkedin thread ini buat lo semua yang lagi cari kerja remote biar gak kena juga	1
6	apes bgt kmrn snder abis ketipu sama jasa hapus akun udh byr 135k eh malah disuruh tf lg dgn alasan server dll udh jelas scam ini hati2 jgn percaya sama jasa pemulihan akun hapus akun di x	1
7	papaku habis ketipu 120 juta karena orang scam ngaku jadi pihak bank ngeprosesnya gimana ya kejadiannya ternyata udah sebulan lalu tapi ortuku pasrah	1
8	jelas banget scam tapi paling ada yang ketipu lagi	1
9	hati2 scam jangan ketipu kalau perlu isi saldo top up atau apapun bahasanya tu udh masuk scam nder awalnya 45rb ntar lama kena puluhan juta karena bonus yg didapet beneran dikirim udh ketipu baru lemes	1
10	scam timothy ni susah buat dibikin delik aduannya aja keitungnya tetep nipu sebenernya tapi lu ga bisa laporin dia karena dia sendiri jg tau celah mana dia bisa bohong dengan aman	1
11	ges tiati dia scam tiket bigu day 2 pertama nama dia agnes sekarang ganti ke dindaa gua udh ketipu dan diblok sama dia capek banget sebenarnya koar koar	1
12	hari ini cuacanya enak banget buat jalan jalan pagi ke taman sama keluarga	0
13	info dong rekomendasi tempat makan seblak yang paling enak di daerah bandung barat	0
14	alhamdulillah akhirnya sidang skripsi selesai juga makasih buat temen temen yang udah bantuin	0
15	semalem nonton pertandingan bola seru banget gila golnya keren abis	0
16	ada yang tau cara benerin laptop yang layarnya tiba tiba blank hitam nggak	0
17	Pohon sakura bermekaran di taman kota. Sepanjang jalan menuju lokasi temu, Shinji baru menyadari cukup banyak penduduk setempat yang beraktivitas di siang hari. Kebanyakan dari mereka menikmati kombinasi langit cerah serta bunga merah muda yang tentu sayang apa	0
18	viral chat diduga karyawan Gacoan Marelan yg mau izin cuti krn ngurus orangtuanya yg masuk rumah sakit, malah dibalas sama HRD nya suruh resign aja.	0
19	kalian ngerasa ga kalo pantura tuh jadi radiator springs-nya pulau jawa semenjak adanya tol trans jawa? yg tinggal di pantura udah gak semeriah dulu kah momentum mudik lebaran?	0
20	Hari ini cuaca panas banget, pengen beli es kopi.	0
21	Apel di Bawah Hujan Usai Libur Lebaran, Bupati Situbondo dan ASN Basah-basahan	0
22	Sinyal provider X hari ini lemot banget sih, padahal kuota masih banyak.	0
23	baru tau ternyata Parfum Dan Skincare Murah bisa semurah ini, apalagi pas crazy brand mega offer s.d 90%, auto kalap dikit	0
24	Akhirnya paket belanjaan dari e-commerce nyampe juga, kurirnya ramah	0
25	Beneran kaget liat harga Parfum Dan Skincare Murah di lazada 4.4 sale, makin untung karena ada crazy brand mega offer s.d 90% dan voucher bonus s.d 500rb, mending langsung amankan di link ini	0
26	Pernah kepikiran gak kenapa akses pendidikan atau pola sistem tertentu terkesan sengaja dibuat stagnan?	0
27	guys percaya gak...Meen nungguin Krating kelar syuting dulu....supaya tetep bisa jalan bareng....	0
28	Mulai banyak game internasional yg tidak lulus rating IGRS	0
29	Komdigi, membatasi akses medsos bagi anak di bawah 16 tahun, tapi lupa batasi medsos utk lansia.	0
30	Pendidikan adalah kunci utama untuk memutus rantai kemiskinan.	0
31	Wajar saja industri mobil mereka menyalip Jepang & Jerman, industri telekomunikasi mereka melibas Samsung (Korea) & IPhone (USA), serta mampu kuasai SDA diseluruh dunia.	0
32	Pada tahap idealnya, pendidikan harus dibebaskan dari kategorisasi subjek pembelajaran.	0

Gambar 4 Data mentah tweet sebelum proses cleaning

Evaluasi dilakukan terhadap dua skenario, yaitu tanpa penerapan SMOTE dan dengan penerapan SMOTE. Pada kedua skenario, SMOTE ditempatkan di dalam subproses pelatihan Cross Validation untuk memastikan data uji tetap berupa data asli, sehingga hasil evaluasi terbebas dari *Data Leakage*. Seluruh metrik dilaporkan dengan kelas penipuan sebagai kelas positif. Hasil komparasi disajikan pada Tabel 1 dan Tabel 2.

Tabel 1 Komparasi algoritma deteksi penipuan (Tanpa SMOTE)

Algoritma Klasifikasi	Akurasi (%)	Presisi (%)	Recall (%)	F-Measure (%)
Naive Bayes	66,67	48,00	90,00	60,76
Support Vector Machine	70,00	N/A	0,00	N/A
Logistic Regression	63,33	0,00	0,00	N/A

Keterangan: N/A menunjukkan nilai tak terdefinisi karena model tidak menghasilkan prediksi positif (TP = FP = 0).

Tabel 2 Komparasi algoritma deteksi penipuan (Dengan SMOTE)

Algoritma Klasifikasi	**Akurasi (%)**	**Presisi (%)**	**Recall (%)**	**F-Measure (%)**
Naive Bayes	66,67	48,33	80,00	58,00
Support Vector Machine	70,00	N/A	0,00	N/A
Logistic Regression	50,00	12,50	10,00	11,76

Keterangan: N/A menunjukkan nilai tak terdefinisi karena model tidak menghasilkan prediksi positif (TP = FP = 0).

Berdasarkan Tabel 1 dan Tabel 2, *Naive Bayes* merupakan satu-satunya algoritma yang konsisten mampu mengenali kelas penipuan. Pada skenario tanpa SMOTE, *Naive Bayes* memperoleh

 ISSN:2302-8149
e-ISSN:2540-9719

recall tertinggi sebesar 90,00% dengan F-Measure 60,76%, yang berarti model berhasil menangkap sebagian besar cuitan penipuan. Setelah penerapan SMOTE, kinerja *Naive Bayes* justru sedikit menurun, dengan recall turun menjadi 80,00% dan F-Measure menjadi 58,00%.

A. Skenario Tanpa SMOTE

Rincian confusion matrix untuk skenario tanpa SMOTE disajikan pada Tabel 3 (*Naive Bayes*), Tabel 4 (*Support Vector Machine*), dan Tabel 5 (*Logistic Regression*).

Tabel 3 Confusion matrix *naive bayes* (tanpa SMOTE)

	Aktual: Penipuan (true)	**Aktual: Bukan (false)**
Prediksi: Penipuan (true)	8 (TP)	9 (FP)
Prediksi: Bukan (false)	1 (FN)	12 (TN)

Recall = 8/(8+1) = 90,00%; Presisi = 8/(8+9) = 48,00%; F-Measure = 60,76%.

Tabel 4 Confusion matrix *support vector machine* (tanpa SMOTE)

	Aktual: Penipuan (true)	**Aktual: Bukan (false)**
Prediksi: Penipuan (true)	0 (TP)	0 (FP)
Prediksi: Bukan (false)	9 (FN)	21 (TN)

Model memprediksi seluruh data sebagai bukan penipuan. Recall = 0/(0+9) = 0,00%; Presisi tak terdefinisi (TP=FP=0). Akurasi 70,00% hanya mencerminkan proporsi kelas mayoritas.

Tabel 5 Confusion matrix *logistic regression* (tanpa SMOTE)

	Aktual: Penipuan (true)	**Aktual: Bukan (false)**
Prediksi: Penipuan (true)	0 (TP)	2 (FP)
Prediksi: Bukan (false)	9 (FN)	19 (TN)

Recall = 0/(0+9) = 0,00%; Presisi = 0/(0+2) = 0,00%; F-Measure tak terdefinisi.

B. Skenario Dengan SMOTE

Rincian Confusion matrix untuk skenario dengan SMOTE disajikan pada Tabel 6 (*Naive Bayes*), Tabel 7 (*Support Vector Machine*), dan Tabel 8 (*Logistic Regression*).

Tabel 6 Confusion matrix *naive bayes* (dengan SMOTE)

	Aktual: Penipuan (true)	**Aktual: Bukan (false)**
Prediksi: Penipuan (true)	7 (TP)	8 (FP)
Prediksi: Bukan (false)	2 (FN)	13 (TN)

Recall = 7/(7+2) = 80,00%; Presisi = 7/(7+8) = 48,33%; F-Measure = 58,00%.

Tabel 7 Confusion matrix *support vector machine* (dengan SMOTE)

	Aktual: Penipuan (true)	**Aktual: Bukan (false)**
Prediksi: Penipuan (true)	0 (TP)	0 (FP)
Prediksi: Bukan (false)	9 (FN)	21 (TN)

Model memprediksi seluruh data sebagai bukan penipuan. Recall = 0,00%; Presisi tak terdefinisi (TP=FP=0).

Tabel 8 Confusion matrix *logistic regression* (dengan SMOTE)

	Aktual: Penipuan (true)	**Aktual: Bukan (false)**
Prediksi: Penipuan (true)	1 (TP)	7 (FP)
Prediksi: Bukan (false)	8 (FN)	14 (TN)

Recall = 1/(1+8) = 11,11% (dibulatkan 10,00% sesuai keluaran rata-rata lipatan); Presisi = 1/(1+7) = 12,50%; F-Measure = 11,76%.

Support Vector Machine memperlihatkan fenomena yang perlu dicermati. Meskipun akurasinya tampak tinggi (70,00%), nilai recall pada kelas penipuan adalah 0,00%, baik dengan maupun tanpa SMOTE. Pemeriksaan confusion matrix menunjukkan bahwa SVM memprediksi seluruh data sebagai bukan-penipuan. Dengan demikian, akurasi 70,00% tersebut semata-mata mencerminkan proporsi

 ISSN:2302-8149
e-ISSN:2540-9719

kelas mayoritas pada data uji, bukan kemampuan model dalam mendeteksi penipuan. Hal ini menegaskan bahwa akurasi merupakan metrik yang menyesatkan pada data tidak seimbang.

Logistic Regression menunjukkan kinerja yang lemah pada kedua skenario, dengan recall hanya 0,00% (tanpa SMOTE) dan 10,00% (dengan SMOTE). Walaupun SMOTE memberikan sedikit perbaikan pada *Logistic Regression*, nilainya tetap jauh di bawah *Naive Bayes*. Ukuran dataset yang kecil turut memengaruhi stabilitas hasil evaluasi. Hal ini tercermin dari nilai simpangan baku antar-lipatan (*standard deviation*) yang relatif besar pada beberapa konfigurasi, misalnya *Logistic Regression* dengan SMOTE pada nilai *recall* sebesar 10,00% memiliki simpangan baku hingga ±22,36%, yang menunjukkan variasi tinggi antar-lipatan. Dengan total data yang terbatas, setiap lipatan uji hanya memuat sejumlah kecil sampel, sehingga perubahan pada beberapa prediksi saja dapat menyebabkan fluktuasi metrik yang besar. Kondisi ini menegaskan bahwa hasil yang diperoleh, meskipun valid secara prosedural, perlu ditafsirkan dengan hati-hati dan belum dapat digeneralisasi secara luas. Ketidakstabilan ini merupakan konsekuensi langsung dari ukuran data, bukan dari kesalahan prosedur evaluasi, dan menjadi alasan utama diperlukannya validasi pada dataset yang lebih besar.

Secara keseluruhan, hasil ini berbeda dengan ekspektasi awal bahwa SMOTE akan meningkatkan kinerja seluruh algoritma. Pada dataset berukuran kecil dengan representasi fitur teks berdimensi tinggi (TF-IDF), sampel sintetis yang dihasilkan SMOTE tidak selalu merepresentasikan pola kelas minoritas secara akurat, sehingga manfaatnya terbatas bahkan dapat sedikit menurunkan kinerja. Temuan ini sejalan dengan sejumlah studi yang melaporkan bahwa efektivitas SMOTE bergantung pada karakteristik dan ukuran data.

5 Kesimpulan

Penelitian ini mengevaluasi kinerja tiga algoritma klasifikasi dalam mendeteksi penipuan digital pada platform X, dengan dan tanpa penerapan SMOTE, menggunakan prosedur evaluasi yang terbebas dari *Data Leakage*. Hasil penelitian menunjukkan bahwa *Naive Bayes* merupakan model paling andal dalam mendeteksi penipuan, dengan recall tertinggi sebesar 90,00% dan F-Measure 60,76% pada skenario tanpa SMOTE. Penerapan SMOTE pada dataset berukuran kecil dan tidak seimbang dalam penelitian ini tidak terbukti meningkatkan kinerja secara konsisten, dan bahkan sedikit menurunkan kinerja *Naive Bayes*. Penelitian ini juga menunjukkan bahwa metrik akurasi dapat menyesatkan pada data tidak seimbang, sebagaimana terlihat pada SVM yang memperoleh akurasi 70,00% namun gagal mendeteksi satu pun kasus penipuan. Oleh karena itu, recall dan F-Measure pada kelas minoritas lebih tepat digunakan sebagai tolok ukur kinerja sistem deteksi penipuan. Secara metodologis, penelitian ini menegaskan pentingnya penempatan SMOTE di dalam subproses pelatihan Cross Validation untuk menghindari estimasi kinerja yang terlalu optimistis akibat *Data Leakage*. Berdasarkan keterbatasan tersebut, penelitian selanjutnya disarankan untuk: (1) memperbesar dan memperkaya dataset melalui pengumpulan cuitan dari berbagai sumber agar pola penipuan dapat dipelajari secara lebih representatif dan hasil evaluasi lebih stabil; (2) mengeksplorasi variasi teknik penyeimbangan data lain, seperti SMOTE-ENN, SMOTE-Tomek, atau *Borderline-SMOTE*, untuk menilai kembali efektivitasnya pada data teks berbahasa Indonesia; dan (3) menempatkan proses ekstraksi fitur TF-IDF sepenuhnya di dalam subproses pelatihan *Cross Validation* sehingga evaluasi benar-benar bebas dari segala bentuk kebocoran data. Ketiga arah ini diharapkan dapat memperkuat validitas dan generalisasi model deteksi penipuan berbasis teks pada penelitian berikutnya.

Referensi

[1] H. Awan Irawan, “Deteksi Fraud Kartu Kredit dengan *Logistic Regression*, *Random Forest*, dan *Gradient Boosting*,” *Jurnal Informatika Terpadu*, Vol. 11, No. 2, pp. 92–97, 2025, [Online]. Available: https://journal.nurulfikri.ac.id/index.php/JIT

[2] Maulana Malik Ibrahim and Sony Alfauzan, “Analisis Kinerja Model *Machine Learning* untuk Mendeteksi Transaksi Fraud pada Sistem Pembayaran Online,” *Jurnal Ilmiah Nusantara*, Vol. 2, No. 3, pp. 35–49, Apr. 2025, DOI: 10.61722/jinu.v2i3.4276.

[3] 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.

[4] Reyhand Ardhitha, Revifal Anugerah, and Tata Sutabri, "Analisis Penerapan *Machine Learning* dan Algoritma Anomali untuk Deteksi Penipuan pada Transaksi Digital," *Repeater : Publikasi Teknik Informatika dan Jaringan*, Vol. 3, No. 1, pp. 80–90, Jan. 2025, DOI: 10.62951/repeater.v3i1.345.

[5] L. Mahya, T. Tarjo, Z. M. Sanusi, and F. A. Kurniawan, "*Intelligent Automation of Fraud Detection and Investigation:A Bibliometric Analysis Approach*," *Jurnal Reviu Akuntansi dan Keuangan*, Vol. 13, No. 3, pp. 588–613, Oct. 2023, DOI: 10.22219/jrak.v13i3.28487.

[6] M. Reyhan, D. Ramadhani Ahmad, N. Ari Ramadhan, R. N. Hidayat, and I. Respati Kusumasari, "Penggunaan Data Analisis dan Big Data dalam Strategi Pengambilan Keputusan Keuangan," 2024. [Online]. Available: https://economics.pubmedia.id/index.php/jampk

[7] A. C. Umami and Y. Yuniseffendri, "Implementasi Makna Intensi dalam Cuitan Akun Twitter Pejabat Negara (Kajian Semantik)," *BAPALA*, Vol. 10, No. 3, 2023.

[8] A. Z. Dilivia, L. Febriyanto, and B. Ginanjar, "Pergeseran Makna Kosakata Flora dalam Metafora di Media Sosial Twitter: Kajian Semantik," *Linguistik Indonesia*, Vol. 41, No. 1, pp. 75–88, 2023.

[9] M. Oktaviana, Z. A. Achmad, H. Arviani, and K. Kusnarto, "Budaya Komunikasi Virtual di Twitter dan Tiktok: Perluasan Makna Kata Estetik," *Satwika: Kajian Ilmu Budaya dan Perubahan Sosial*, Vol. 5, No. 2, pp. 173–186, 2021.

[10] A. Tri Arsanto, A. Faizin, M. Lutfi, Z. Nikmatus Saadah, T. informatika, and U. Yudharta Pasuruan, "Sistemasi: Jurnal Sistem Informasi Optimasi Algoritma *Naive Bayes* dengan Kombinasi SMOTETomek untuk *Imbalance Class Fraud Detection Optimization of the Naive Bayes Algorithm with SMOTETomek Combination for Imbalance Class Fraud Detection*." [Online]. Available: http://sistemasi.ftik.unisi.ac.id

[11] T. Berhane, T. Melese, A. Walelign, and A. Mohammed, "*A Hybrid Convolutional Neural Network and Support Vector Machine-based Credit Card Fraud Detection Model*," *Math. Probl. Eng.*, Vol. 2023, No. 1, Jan. 2023, DOI: 10.1155/2023/8134627.

[12] J. R. Sari, K. Sadik, A. M. Soleh, and C. Suhaeni, "Evaluasi Model Klasifikasi dalam Deteksi Penipuan Transaksi: Studi Kasus pada Data Tidak Seimbang," *Jurnal Gaussian*, Vol. 14, No. 2, pp. 565–576, Dec. 2025, DOI: 10.14710/j.gauss.14.2.565-576.

[13] R. Bounab, K. Zarour, B. Guelib, and N. Khlifa, "*Enhancing Medicare Fraud Detection Through Machine Learning: Addressing Class Imbalance with SMOTE-ENN*," *IEEE Access*, Vol. 12, pp. 54382–54396, 2024, DOI: 10.1109/ACCESS.2024.3385781.

[14] Z. Zhao and T. Bai, "*Financial Fraud Detection and Prediction in Listed Companies using SMOTE and Machine Learning Algorithms*," *Entropy*, Vol. 24, No. 8, Aug. 2022, DOI: 10.3390/e24081157.

[15] D. R. K. Saputra, Y. V. Via, and A. N. Sihananto, "Deteksi Anomali menggunakan *Ensemble Learning* dan *Random Oversampling* pada Penipuan Transaksi Keuangan," *Jurnal Informatika dan Teknik Elektro Terapan*, Vol. 12, No. 3, Aug. 2024, DOI: 10.23960/jitet.v12i3.4910.

[16] A. M. Syahbani, W. Firdaus, and K. A. Musodo, "*A Comparative Study of Data Mining Algorithms for Fraud Detection in Financial Transactions*," *Sinkron*, Vol. 9, No. 2, pp. 814–821, Apr. 2025, DOI: 10.33395/sinkron.v9i2.14645.