Building of Informatics, Technology and Science (BITS)
Volume 6, No 2, Desember 2024 Page: 1427−1439
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i3.6110

Penerapan Metode *Supervised Learning* dan Teknik *Resampling* untuk Prediksi Penipuan Transaksi Keuangan

Elven Constancio, Ken Ditha Tania*

Fakultas Ilmu Komputer, Program Studi Sistem Informasi, Universitas Sriwijaya, Kota Palembang, Indonesia
Email: [1]elven.constancio04@gmail.com, [2,*]kenya.tania@gmail.com
Email Penulis Korespondensi: kenya.tania@gmail.com
Submitted: **21/10/2024**; Accepted: **01/12/2024**; Published**: 03/12/2024**

Abstrak−Penipuan transaksi keuangan dapat mengakibatkan konsekuensi yang menghancurkan bagi stabilitas perusahaan, serta kerugian besar bagi pemegang saham, industri, dan bahkan pasar secara keseluruhan. Seiring dengan meningkatnya penipuan dalam transaksi keuangan, dibutuhkan metode yang efektif untuk mendeteksi dan mencegah aktivitas penipuan secara akurat. Penelitian ini bertujuan untuk membandingkan kinerja lima model pembelajaran mesin, yaitu *Random Forest*, *K-Nearest Neighbors* (KNN), *Decision Tree*, *XGBoost*, dan *Extra Trees*, dalam mendeteksi penipuan transaksi keuangan yang menggunakan dataset tidak seimbang. Untuk mengatasi masalah ketidakseimbangan data, diterapkan tiga teknik *resampling*, yakni *Synthetic Minority Oversampling Technique* (SMOTE), *Adaptive Synthetic Sampling* (ADASYN), dan *Undersampling*. Eksperimen dilakukan dengan dua rasio pembagian data latih dan data uji, yaitu 70:30 dan 80:20. Hasil evaluasi menunjukkan bahwa model XGBoost adalah model yang paling konsisten, dengan nilai ROC AUC tertinggi yaitu 99%, terutama setelah penerapan teknik *resampling*. Rasio data 80:20 menghasilkan distribusi yang lebih seimbang serta performa model yang lebih baik dalam mendeteksi kelas minoritas terutama setelah teknik *resampling*. Hasil Penelitian ini menunjukkan bahwa model *XGBoost* dengan teknik *resampling* sangat efektif dalam mengatasi ketidakseimbangan data.

Kata Kunci: Penipuan Transaksi Keuangan; SMOTE; ADASYN; Undersampling; XGBoost

Abstract−Financial transaction fraud can result in devastating consequences for the stability of companies, as well as huge losses for shareholders, the industry, and even the market as a whole. As fraud in financial transactions increases, there is a need for effective methods to accurately detect and prevent fraudulent activities. This study aims to compare the performance of five machine learning models, namely Random Forest, K-Nearest Neighbors (KNN), Decision Tree, XGBoost, and Extra Trees, in detecting financial transaction fraud using an imbalanced dataset. To overcome the data imbalance problem, three resampling techniques are applied, namely Synthetic Minority Oversampling Technique (SMOTE), Adaptive Synthetic Sampling (ADASYN), and Undersampling. Experiments were conducted with two training and test data sharing ratios, namely 70:30 and 80:20. The evaluation results showed that the XGBoost model was the most consistent, with the highest ROC AUC value of 99%, especially after the application of resampling techniques. The 80:20 data ratio resulted in a more balanced distribution and better model performance in detecting the minority class, particularly after resampling. This study concludes that the XGBoost model with resampling techniques is highly effective in addressing data imbalance.

Keywords: Financial Transaction Fraud; SMOTE; ADASYN; Undersampling; XGBoost

1. PENDAHULUAN

Masalah penipuan dalam transaksi keuangan terus meningkat dalam beberapa tahun terakhir, yang juga berdampak buruk pada kepercayaan di antara para pelaku bisnis dan pelaku pasar [1]. Penipuan transaksi keuangan dapat mengakibatkan konsekuensi yang menghancurkan bagi stabilitas perusahaan, serta kerugian besar bagi pemegang saham, industri, dan bahkan pasar secara keseluruhan [2]. Seiring dengan meningkatnya penipuan dalam transaksi keuangan, dibutuhkan metode yang efektif untuk mendeteksi dan mencegah aktivitas penipuan secara akurat. Salah satu masalah utama dalam mendeteksi penipuan transaksi keuangan adalah ketidakseimbangan data, di mana jumlah transaksi non penipuan secara signifikan jauh lebih tinggi dibandingkan dengan jumlah transaksi penipuan. Ketidakseimbangan ini dapat mengakibatkan model lebih cenderung memprediksi transaksi sah dan gagal mendeteksi transaksi penipuan dengan baik. Untuk mengatasi masalah ketidakseimbangan ini, teknik *resampling* seperti *oversampling data* menggunakan *Synthetic Minority Oversampling Technique* (SMOTE) dapat diterapkan untuk meningkatkan proporsi transaksi penipuan dalam dataset, sehingga memungkinkan model untuk mempelajari pola dari data yang lebih proporsional [3]. Selain *oversampling* SMOTE, teknik *Adaptive Synthetic Sampling* (ADASYN) juga diterapkan pada penelitian ini. ADASYN memanfaatkan distribusi kepadatan sebagai dasar untuk secara otomatis menetapkan jumlah sampel sintetik yang diperlukan bagi setiap contoh data minoritas [4]. Selain *oversampling*, juga digunakan teknik *undersampling* yaitu dengan menghapus sampel dari kelas mayoritas [5].

Penelitian ini menggunakan beberapa model pembelajaran mesin untuk mendeteksi penipuan transaksi keuangan, yaitu *Random Forest*, *K-Nearest Neighbors* (KNN), *Decision Tree*, *XGBoost*, dan *Extra Trees* (*Extremely Randomized Trees*). Model – model ini dipilih karena masing – masing memiliki kemampuan untuk menangani masalah klasifikasi dan ketidakseimbangan data. *Random Forest*, model ensemble berbasis pohon keputusan, yang terinspirasi oleh ruang acak dan pemilihan pemisahan acak [6]. Algoritma KNN menghasilkan prediksi model dengan mengambil suara terbanyak dari K titik data terdekat dengan titik uji sebagai dasar umpan balik [7]. *Decision tree* adalah suatu metode yang digunakan alam analisis data untuk melakukan klasifikasi dan regresi [8]. *XGBoost* dipilih karena kemampuannya dalam menangani data yang tidak seimbang dan *overfitting*. *XGBoost* termasuk dalam kategori pembelajaran *ensemble* yang menggabungkan beberapa pohon keputusan (*decision trees*) untuk menghasilkan

Building of Informatics, Technology and Science (BITS)
Volume 6, No 2, Desember 2024 Page: 1427−1439
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i3.6110

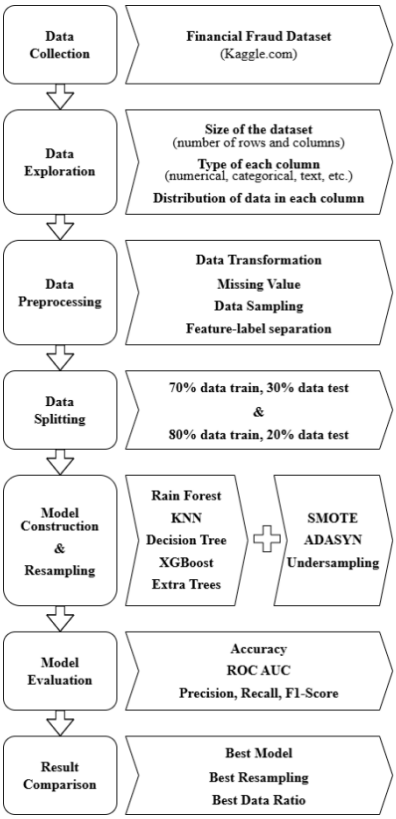
prediksi yang lebih baik [9]. Terakhir, *Extra Trees* dikenal karena kecepatan dan ketepatan, terutama dalam menangani kumpulan data yang sangat besar [10]. Hasil dari semua model ini akan dibandingkan untuk mengevaluasi efektivitas masing – masing dalam mendeteksi tindakan penipuan. Hasil ini dapat memberikan wawasan yang berharga untuk memilih pendekatan yang paling sesuai untuk menangani masalah penipuan transaksi keuangan.

Penelitian terdahulu yang dilakukan oleh Faried Zamachsari dan Niken Puspitasari pada tahun 2021, menerapkan *Deep Learning* dan teknik *resampling* SMOTE dalam deteksi penipuan transaksi keuangan. Hasil penelitian menunjukkan bahwa resampling SMOTE efektif dalam mengatasi ketidakseimbangan data, dan model *Extra Trees* memberikan performa yang optimal [11]. Selanjutnya, pada tahun 2024, penelitian tentang deteksi penipuan kartu kredit oleh Lailan Sahrina Hasibuan dan Fatimah Alfiatul Jannah menemukan bahwa dengan teknik *resampling* ADASYN dan optimasi parameter yang tepat, model SVM mendapatkan performa paling baik dibandingkan model lainnya bahkan pada dataset yang tidak seimbang [12]. Penelitian lainnya oleh Mukhlis Febriady, Samsuryadi, dan Dian Palupi Rini pada tahun 2022 membahas tentang klasifikasi transaksi penipuan pada kartu kredit. Hasilnya menunjukkan bahwa Random Forest memberikan kinerja terbaik dalam semua pengujian, terutama saat digabungkan dengan *resampling* SMOTE [13]. Selanjutnya penelitian oleh Wowon Priatna pada tahun 2024 yang menganalisis dampak pengambilan sampel data untuk mengoptimalkan data yang tidak seimbang pada klasifikasi penipuan pada transaksi *E-Commerce*, menunjukkan bahwa algoritma *Synthetic Minority Over Sampling Technique* (SMOTE) berhasil menyeimbangkan data dengan metode C45 menjadi yang paling efektif [14]. Penelitian lainnya yang dilakukan oleh Kurniabudi, Abdul Harris, dan Veronica, tentang pendeteksian anomali pada data dengan dimensi tinggi dan distribusi yang tidak seimbang menunjukkan bahwa *Random Tree* dan *Random Forest* memiliki performa yang sangat baik dalam mendeteksi anomali [15].

Penelitian ini bertujuan untuk menguji dan membandingkan beberapa model pembelajaran mesin seperti *Random Forest*, *K-Nearest Neighbors* (KNN), *Decision Tree*, *XGBoost*, dan *Extra Trees* untuk mendeteksi penipuan dengan menerapkan teknik resampling *Synthetic Minority Oversampling Technique* (SMOTE), *Adaptive Synthetic Sampling* (ADASYN), dan *Undersampling* guna mengatasi ketidakseimbangan data dalam dataset transaksi keuangan. Penelitian ini diharapkan mampu memberikan kontribusi signifikan dalam pengembangan metode deteksi penipuan yang lebih efektif dan efisien, serta membantu organisasi dalam mengurangi risiko dan kerugian akibat penipuan transaksi keuangan. Selain itu, hasil dari penelitian ini diharapkan dapat menjadi referensi bagi penelitian selanjutnya dalam bidang ini.

2. METODOLOGI PENELITIAN

Penelitian ini melibatkan beberapa tahap yang dilakukan untuk mencapai tujuan yang telah ditetapkan [3]. Gambar 1 di bawah ini mengilustrasikan keseluruhan tahapan penelitian dari awal hingga akhir.



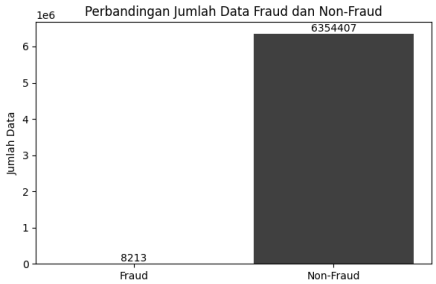
Gambar 1. Tahapan Penelitian

Building of Informatics, Technology and Science (BITS)
Volume 6, No 2, Desember 2024 Page: 1427−1439
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i3.6110

Penelitian ini diawali dengan Pengumpulan Data (*Data Collection*), kemudian dilanjutkan dengan Eksplorasi Data (*Data Exploration*) untuk memahami karakteristik data. Tahap berikutnya adalah Pra-pemrosesan Data (*Preprocessing Data*) dengan pemeriksaan *missing value*, pengambilan *data sampling*, yang dilanjutkan dengan Pembagian Data (*Data Splitting*) ke dalam subset pelatihan dan pengujian dengan dua rasio yaitu 70:30 dan 80:20. Setelah pembagian data, dilakukan proses Evaluasi Model dengan menggunakan *Random Forest*, KNN (*K-Nearest Neighbors*), *Decision Tree*, *XGBoost* (*Extreme Gradient Boosting*), dan *Extra Trees* (*Extremely Randomized Trees*), serta dilakukan teknik *Resampling* SMOTE (*Synthetic Minority Oversampling Technique Strategy*), ADASYN (*Adaptive Synthetic Sampling*), dan *Undersampling* untuk mengatasi masalah ketidakseimbangan data. Tahap terakhir adalah Perbandingan Hasil dari beberapa model yang telah dievaluasi untuk ditentukan model yang terbaik, *resampling* terbaik, dan rasio data yang bagus untuk digunakan.

2.1 Dataset

Dataset yang digunakan dalam penelitian ini berisi data transaksi keuangan yang terdiri dari beberapa variabel, seperti *step* (urutan waktu dan langkah dalam transaksi), *type* (tipe pembayaran), *amount* (nominal), *nameOrig* (nama pengirim), *oldbalanceOrg* (saldo awal pengirim), *newbalanceOrig* (saldo akhir pengirim), *nameDest* (nama penerima), *oldbalanceDest* (saldo awal penerima), *newbalanceDest* (saldo akhir penerima), *isFraud* (penipuan), *isFlaggedFraud* (berpotensi penipuan).

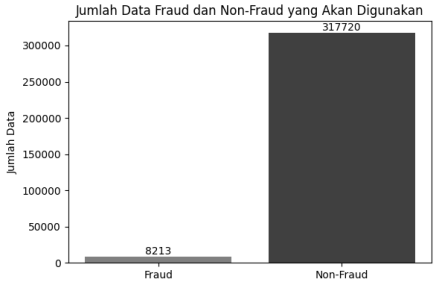


Gambar 2. Grafik Perbandingan Jumlah Data *Fraud* dan *Non-Fraud*

Gambar 2 menampilkan grafik perbandingan dataset antara data penipuan (*fraud*) dan non-penipuan (*non-fraud*), yang proporsi datanya sangat tidak seimbang dengan data non-penipuan yang mendominasi. Jumlah datanya sebanyak 6.362.620 dataset transaksi yang terdiri dari 8.213 data penipuan dan 6.354.407 data non penipuan dari https://www.kaggle.com/datasets/sriharshaeedala/financial-fraud-detection-dataset.

2.2 *Preprocessing Data*

Langkah awal dalam proses *preprocessing* data adalah memastikan bahwa tidak ada data yang kosong (*null*). Berdasarkan pemeriksaan menggunakan fungsi isnull(), tidak ditemukan adanya nilai yang hilang. Dikarenakan adanya ketidakseimbangan data antara data penipuan dan non-penipuan, maka diambil sampel sebesar 5% dari keseluruhan data non-penipuan, sementara semua data penipuan digunakan sebagai sampel. Hal ini bertujuan untuk mencegah lamanya proses pencarian parameter optimum akibat ukuran data asli yang besar [12]. Setelah pengambilan sampel, data digabungkan untuk membentuk dataset baru yang dapat dilihat pada Gambar 3.



Gambar 3. Grafik Perbandingan Jumlah Data *Fraud* dan *Non-Fraud* yang Akan Digunakan

Gambar 3 menampilkan grafik perbandingan jumlah data penipuan (*fraud*) dan non-penipuan (*non-fraud*) dengan total penipuan sebanyak 8.213 data dan non-penipuan sebanyak 26.487 data. Selanjutnya, fitur kategorikal, yaitu variabel *type*, yang terdiri dari *Cash In*, *Cash Out*, *Debit*, *Payment*, dan *Transfer*, diubah menjadi variabel *dummy*. Proses ini menghasilkan variabel biner (0 dan 1), yang diperlukan karena beberapa algoritma pembelajaran mesin tidak dapat menangani data kategorikal secara langsung.

Building of Informatics, Technology and Science (BITS)
Volume 6, No 2, Desember 2024 Page: 1427−1439
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i3.6110

2.3 *Splitting Data*

Pada tahap ini, variabel fitur (X) dipisahkan dari variabel target (y). Variabel fitur terdiri dari semua kolom dalam dataset kecuali kolom *isFraud*, *isFlaggedFraud*, *nameOrig*, dan *nameDest*, yang dihapus karena tidak relevan untuk proses pelatihan model. Sementara itu, kolom *isFraud* digunakan sebagai variabel target (y), yang menunjukkan apakah suatu transaksi dikategorikan sebagai penipuan atau tidak. Dengan pemisahan ini, model dapat dilatih untuk memprediksi kemungkinan terjadinya penipuan berdasarkan fitur – fitur yang ada dalam dataset.

Lalu dataset dibagi menjadi dua kelompok, yaitu data latih dan data uji. Pembagian dataset sering kali dilakukan oleh para peneliti dengan menggunakan berbagai rasio data latih dan data uji. Misalnya, Liang dkk. (2020) menggunakan rasio 70% data latih dan 30% data uji [16]. Lalu, Ramadina dkk. (2024) menggunakan rasio 80% data latih dan 20% data uji [17]. Pada penelitian ini, pembagian data dilakukan menggunakan dua rasio data latih dan data uji yang berbeda, yaitu 70:30 dan 80:20. Pembagian ini bertujuan untuk mengevaluasi performa model dengan tingkat generalisasi yang lebih baik pada data uji yang tidak digunakan dalam proses pelatihan. Dengan membandingkan kedua rasio ini, diharapkan dapat ditemukan kombinasi yang optimal dalam memaksimalkan akurasi dan kemampuan model dalam mendeteksi penipuan.

2.4 *Resampling Data*

Dalam tahap ini, dilakukan teknik *resampling* untuk mengatasi ketidakseimbangan data antara kelas penipuan dan non-penipuan. Tiga metode yang digunakan dalam penelitian ini adalah SMOTE (*Synthetic Minority Over-sampling Technique*), ADASYN (*Adaptive Synthetic Sampling*), dan *Undersampling*. Hasil *Resampling* yang diterapkan pada data latih dengan rasio 70:30 dan 80:20 tentu akan menghasilkan jumlah data yang berbeda.

2.4.1 SMOTE (*Synthetic Minority Oversampling Technique Strategy*)

SMOTE adalah suatu teknik *oversampling* yang secara khusus dirancang untuk menangani masalah ketidakseimbangan data. Teknik ini menghasilkan sampel sintetis dari kelas minoritas untuk menyeimbangkan distribusi data sehingga memungkinkan distribusi data menjadi lebih seimbang dan mendukung performa model yang lebih baik dalam mendeteksi kelas minoritas [18].

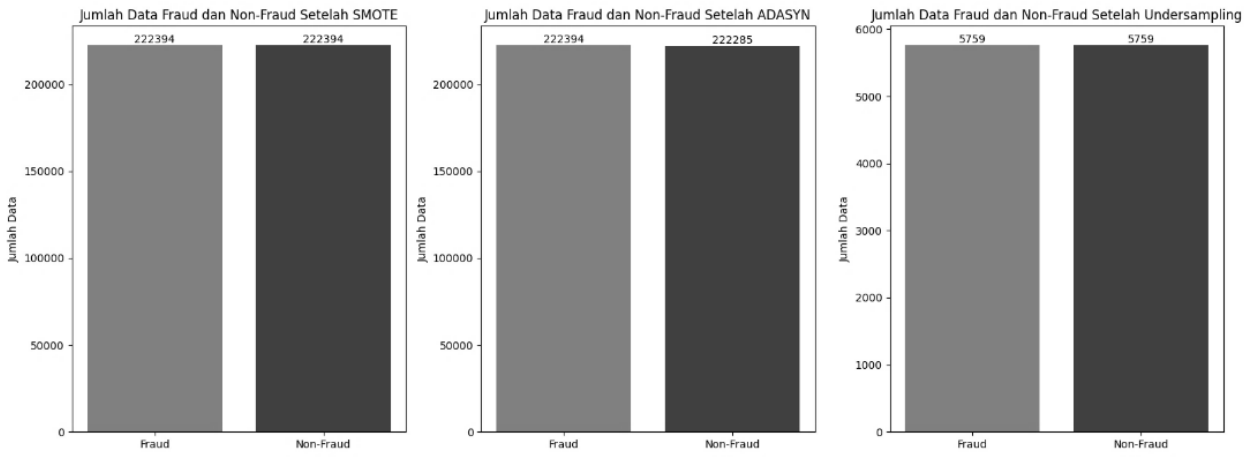
2.4.2 ADASYN (*Adaptive Synthetic Sampling*)

ADASYN merupakan peningkatan dari SMOTE, yang bertujuan untuk mencegah terjadinya *overfitting* akibat penambahan salinan identik dari data minoritas ke dalam dataset utama. ADASYN adalah teknik yang menghasilkan contoh baru dari kelas minoritas tetapi dengan penekanan pada contoh yang lebih sulit untuk diprediksi [19].

2.4.3 *Undersampling*

Undersampling adalah teknik mengurangi jumlah data dari kelas mayoritas untuk mencapai keseimbangan dengan kelas minoritas. Teknik ini dilakukan dengan secara acak mengurangi data dari kelas mayoritas hingga jumlahnya sebanding dengan kelas minoritas [20].

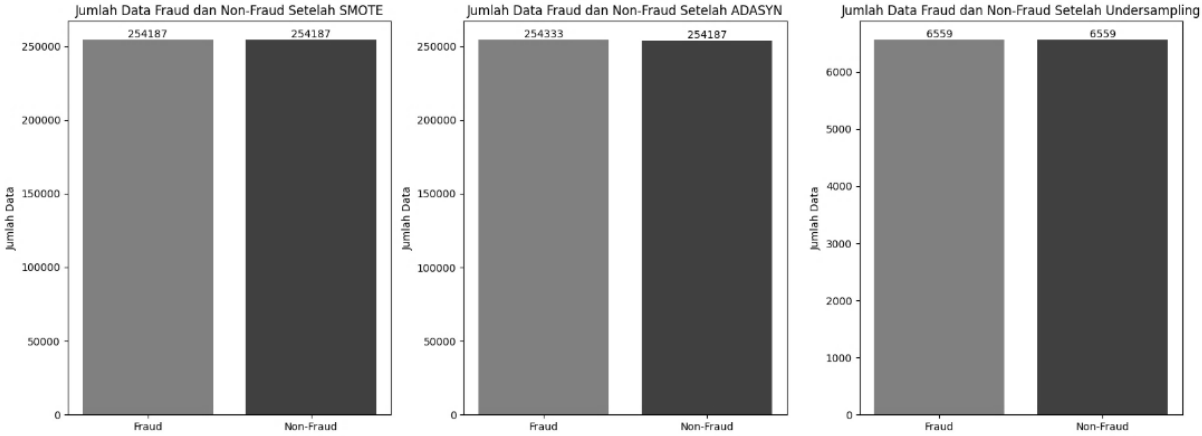
Grafik perbandingan jumlah data setelah SMOTE, setelah ADASYN, dan setelah *Undersampling* untuk rasio 70:30 dan 80:20 dapat dilihat pada Gambar 4 dan 5.



Gambar 4. Grafik Perbandingan Jumlah Data *Fraud* dan *Non-Fraud* Setelah SMOTE, ADASYN, dan *Undersampling* (Rasio 70:30)

Pada data latih dengan rasio 70:30, penerapan SMOTE menghasilkan jumlah data sebanyak 444.788 dengan 222.394 data kelas *fraud* dan 222.394 data kelas *non-fraud*. Untuk ADASYN, jumlah data yang dihasilkan adalah 444.679 dengan 222.394 data kelas *fraud* dan 222.285 data kelas *non-fraud*. Setelah penerapan *undersampling*, jumlah data yang dihasilkan adalah 11.518 dengan 5.759 data kelas *fraud* dan 5759 data kelas *non-fraud*.

Building of Informatics, Technology and Science (BITS)
Volume 6, No 2, Desember 2024 Page: 1427−1439
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i3.6110



Gambar 5. Grafik Perbandingan Jumlah Data *Fraud* dan *Non-Fraud* Setelah SMOTE, ADASYN, dan *Undersampling* (Rasio 80:20)

Pada data latih dengan rasio 80:20, jumlah data setelah penerapan SMOTE adalah 508.374 dengan 254.187 data kelas *fraud* dan 254.187 data kelas *non-fraud*, sedangkan ADASYN adalah 508.520 dengan 254.333 data kelas *fraud* dan 254.187 data kelas *non-fraud*, lalu *undersampling* adalah 13.118 dengan 6.559 data kelas fraud dan 6.559 data kelas non-fraud.

2.5 Pembangunan Model

Pada tahap ini, dilakukan pembangunan model untuk mendeteksi penipuan dalam transaksi keuangan menggunakan berbagai algoritma pembelajaran mesin. Algoritma yang digunakan meliputi *Random Forest*, *K-Nearest Neighbors* (KNN), *Decision Tree*, *XGBoost*, dan *Extra Trees*. Setiap algoritma dipilih karena memiliki keunggulan dan karakteristik yang berbeda dalam menangani masalah klasifikasi, khususnya dalam mendeteksi penipuan dengan data yang tidak seimbang.

2.5.1 *Random Forest*

Random Forest adalah *a*lgoritma *ensemble* yang membentuk beberapa pohon keputusan (*decision tree*) selama proses pelatihan, kemudian menggabungkan hasil dari setiap pohon untuk meningkatkan akurasi prediksi. Keunggulan metode ini terletak pada kemampuannya untuk mencegah *overfitting* secara efektif melalui pengambilan sampel acak dan seleksi fitur [21].

2.5.2 *K-Nearest Neighbors* (KNN)

KNN merupakan metode *supervised learning* yang sederhana. KNN melakukan prediksi dengan melihat tetangga – tetangga terdekat dari data yang diuji. Namun KNN memiliki tantangan dalam menangani data besar. Selain itu, KNN juga memiliki kelemahan dalam hal sensitivitas terhadap data bising (*noisy data*), terutama ketika jumlah tetangga yang dipilih kecil [22].

2.5.3 *Decision Tree*

Decision Tree adalah metode klasifikasi berbasis pohon di mana setiap jalur dari akar menggambarkan urutan pemisahan data hingga mencapai hasil *boolean* di simpul daun. *Decision Tree* adalah representasi hierarkis dari hubungan pengetahuan yang terdiri dari simpul dan cabang [23].

2.5.4 *XGBoost* (*Extreme Gradient Boosting*)

XGBoost merupakan algoritma *boosting* yang sangat kuat dan efisien dalam menangani data dengan ketidakseimbangan kelas. *XGBoost* bekerja dengan cara meningkatkan performa model secara bertahap dengan menambah pohon keputusan baru yang memfokuskan pada kesalahan prediksi dari pohon sebelumnya. Algoritma ini dikenal karena kecepatan dan performanya yang sangat baik pada berbagai jenis data [24].

2.5.5 *Extra Trees* (*Extremely Randomized Trees*)

Mirip dengan *Random Forest*, *Extra Trees* merupakan metode *ensemble learning* yang menggabungkan prediksi dari beberapa *Decision Tree* untuk meningkatkan akurasi dan mengurangi kompleksitas komputasi. Teknik ini bertujuan untuk menurunkan *varians* dalam prediksi dengan membentuk model yang lebih beragam [25].

2.6 Evaluasi Model

Setelah model dilatih, langkah selanjutnya adalah melakukan evaluasi untuk menilai kinerja setiap model dalam mendeteksi penipuan transaksi keuangan. Evaluasi dilakukan dengan menggunakan data uji yang belum pernah

Building of Informatics, Technology and Science (BITS)
Volume 6, No 2, Desember 2024 Page: 1427−1439
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i3.6110

dikenali oleh model sebelumnya, sehingga dapat memberikan pemahaman yang lebih akurat mengenai kemampuan model dalam memprediksi. Beberapa evaluasi yang digunakan dalam penelitian ini meliputi:

a. *Confusion Matrix*: merupakan tabel yang berfungsi untuk mendeskripsikan kinerja model klasifikasi dengan membandingkan prediksi model terhadap label sebenarnya. Tabel ini terdiri dari empat komponen utama yaitu *True Positive* (TP), *True Negative* (TN), *False Positive* (FP), *False Negative* (FN) [26]. *Confusion Matrix* dapat dilihat pada Tabel 1.

Tabel 1. *Confusion Matrix*

	Prediksi Positif	**Prediksi Negatif**
Aktual Positif	*True Positive* (TP)	*True Negative* (TN)
Aktual Negatif	*False Positive* (FP)	*False Negative* (FN)

b. *Accuracy*: digunakan untuk mengukur proporsi prediksi yang benar terhadap total prediksi. Metrik ini memberikan gambaran menyeluruh tentang seberapa efektif model dapat mengklasifikasikan data [10]. Untuk menghitung *accuracy*, dapat menggunakan formula pada persamaan (1).

$$\textbf{\textit{Accuracy}} = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

c. *Precision*: digunakan untuk mengukur proporsi prediksi positif yang benar terhadap total prediksi positif. Metrik ini penting dalam konteks penipuan, karena harus meminimalkan jumlah *false positive* [26]. Untuk menghitung *precision*, dapat menggunakan formula pada persamaan (2).

$$\textbf{\textit{Precision}} = \frac{TP}{TP+FP} \quad (2)$$

d. *Recall*: digunakan untuk mengukur proporsi prediksi positif yang benar terhadap total kasus positif yang sebenarnya [26]. Metrik ini sangat relevan untuk mendeteksi penipuan, karena tujuan utamanya adalah menangkap sebanyak mungkin transaksi yang benar – benar penipuan. Untuk menghitung *recall*, dapat menggunakan formula pada persamaan (3).

$$\textbf{\textit{Recall}} = \frac{TP}{TP+FN} \quad (3)$$

e. *F1-Score*: merupakan rata – rata harmonis antara *precision* dan *recall*, yang menciptakan keseimbangan di antara keduanya. Metrik ini berguna untuk mengevaluasi model ketika terdapat ketidakseimbangan antara kelas positif dan negatif [26]. Untuk menghitung *F1-Score*, dapat menggunakan formula pada persamaan (4).

$$\textbf{\textit{F1-Score}} = 2 \times \frac{Precision \times Recall}{Precision+Recall} \quad (4)$$

f. *Area Under Curve* (AUC): bergungsi untuk mengukur kemampuan model dalam membedakan antara kelas positif dan negatif. AUC yang hampir mencapai 1 menunjukkan bahwa model memiliki kemampuan yang sangat efektif dalam klasifikasi [26].

Setelah menghitung metrik – metrik tersebut, hasil evaluasi dari masing – masing model dibandingkan untuk menentukan model yang paling efektif dalam mendeteksi penipuan. Dengan cara ini, diharapkan dapat diidentifikasi model yang memberikan kinerja terbaik dan dapat diandalkan dalam mendeteksi penipuan transaksi keuangan.

3. HASIL DAN PEMBAHASAN

Pada penelitian ini, telah dilakukan serangkaian eksperimen untuk mengevaluasi kinerja berbagai algoritma pembelajaran mesin dalam mendeteksi penipuan transaksi keuangan. Model – model yang diuji mencakup *Random Forest*, *K-Nearest Neighbors* (KNN), *Decision Tree*, *XGBoost*, dan *Extra Trees*. Evaluasi dilakukan pada data uji 70:30 dan 80:20, baik sebelum dilakukan *resampling* maupun sesudah penerapan *resampling*: SMOTE, ADASYN, dan *Undersampling*. Data yang digunakan pada penelitian ini ditampilkan pada Tabel 2.

Tabel 2. *Dataset*

No.	step	type	amount	oldbalanceOrg	newbalanceOrig	oldBalanceDest	newBalanceDest	isFraud
1	1	*Transfer*	181.00	181.00	0.00	0.00	0.00	1
2	1	*CashOut*	181.00	181.00	0.00	21182.00	0.00	1
3	1	*Transfer*	2806.00	2806.00	0.00	0.00	0.00	1
...	...	...	...	...	...	...	...	...
325932	322	*CashIn*	24684.73	1041724.21	1066408.93	13756291.51	13731606.78	0
325933	379	*CashOut*	94015.56	0.00	0.00	711463.82	805479.38	0

Tabel 2 menunjukkan sampel data yang digunakan dalam penelitian ini untuk mendeteksi penipuan transaksi keuangan. Data mencakup informasi mengenai jenis transaksi, jumlah uang yang terlibat, saldo rekening asal dan

Building of Informatics, Technology and Science (BITS)
Volume 6, No 2, Desember 2024 Page: 1427−1439
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i3.6110

tujuan sebelum dan sesudah transaksi, serta label yang menunjukkan apakah transaksi tersebut merupakan penipuan (*isFraud* = 1) atau bukan (*isFraud* = 0).

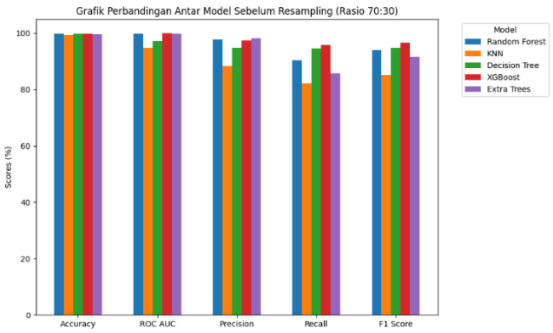
3.1 Hasil Klasifikasi Sebelum Metode *Resampling*

Pada bagian ini, dilakukan pengujian model pembelajaran mesin sebelum menerapkan metode *resampling* untuk menangani ketidakseimbangan data. Pengujian dilakukan dengan dua rasio pembagian data latih dan data uji, yaitu 70:30 dan 80:20. Setiap model, mulai dari *Random Forest*, *K-Nearest Neighbors* (KNN), *Decision Tree*, *XGBoost*, hingga *Extra Trees*, dievaluasi berdasarkan *Accuracy*, *Precision*, *Recall*, *F1-Score*, dan *ROC AUC*.

a. Rasio 70:30: hasil evaluasi klasifikasi pada data uji dengan rasio pembagian 70:30 sebelum *resampling* ditampilkan pada Tabel 3 dan Gambar 6.

Tabel 3. Hasil Klasifikasi Sebelum *Resampling* (Rasio 70:30)

Model	*Accuracy*	*ROC AUC*	*Precision*	*Recall*	*F1-Score*
Random Forest	99,7044	99,8066	97,7082	90,3423	93,881
KNN	99,279	99,8086	88,4058	82,0293	85,0983
Decision Tree	99,7331	97,2032	94,81	94,5395	94,6746
XGBoost	**99,8251**	**99,8743**	97,2671	**95,7213**	**96,488**
Extra Trees	99,6032	99,7299	**98,181**	85,7783	91,5615



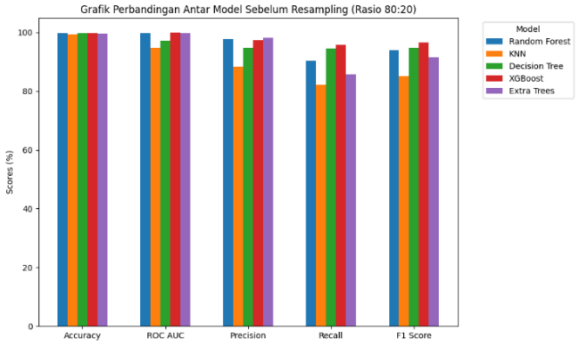
Gambar 6. Grafik Perbandingan Antar Model Sebelum *Resampling* (Rasio 70:30)

Pada Tabel 3 dan Gambar 6 menunjukkan hasil evaluasi pada rasio data 70:30 sebelum *resampling*, model *XGBoost* mendapatkan *accuracy*, *ROC AUC*, *recall*, dan *F1-Score* paling baik dibandingkan model lain. Namun, untuk metrik *precision*, model *Extra Trees* mendapatkan *score* paling tinggi untuk data sebelum *resampling* ini.

b. Rasio 80:20: hasil evaluasi klasifikasi pada data uji dengan rasio pembagian 80:20 sebelum *resampling* ditampilkan pada Tabel 4 dan Gambar 7.

Tabel 4. Hasil Klasifikasi Sebelum *Resampling* (Rasio 80:20)

Model	*Accuracy*	*ROC AUC*	*Precision*	*Recall*	*F1-Score*
Random Forest	99,7239	99,8863	97,6714	91,2938	94,375
KNN	99,2943	94,7916	88,4665	83,0109	85,6519
Decision Tree	99,7806	97,4732	96,2645	95,0423	95,6495
XGBoost	**99,8251**	**99,9733**	97,2393	**95,8283**	**96,5286**
Extra Trees	99,618	99,7901	**98,1494**	86,578	92,0013



Gambar 7. Grafik Perbandingan Antar Model Sebelum *Resampling* (Rasio 80:20)

Building of Informatics, Technology and Science (BITS)
Volume 6, No 2, Desember 2024 Page: 1427−1439
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i3.6110

Pada Tabel 4 dan Gambar 7 terlihat bahwa hasil evaluasi sama seperti pada rasio 70:30, model *XGBoost* masih mendapatkan *score* paling baik untuk metrik *accuracy*, *ROC AUC*, *recall*, dan *F1-Score* dibandingkan model lain. Namun, model *Extra Trees* mendapatkan *score* tertinggi untuk metrik *precision*.

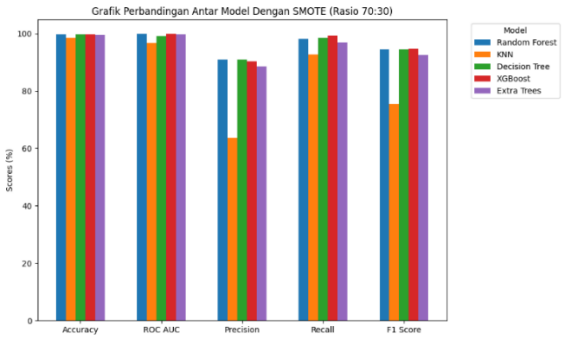
3.2 Hasil Klasifikasi Dengan *Resampling* SMOTE

Dalam tahap pengujian kedua, pengujian model dilakukan dengan teknik *resampling* SMOTE. Pengujian dilakukan dengan dua rasio pembagian data seperti sebelumnya, yaitu 70:30 dan 80:20.

a. Rasio 70:30: hasil evaluasi klasifikasi pada data uji dengan rasio pembagian 70:30 dengan teknik *resampling* SMOTE ditampilkan pada Tabel 5 dan Gambar 8.

Tabel 5. Hasil Klasifikasi Dengan *Resampling* SMOTE (Rasio 70:30)

Model	*Accuracy*	*ROC AUC*	*Precision*	*Recall*	*F1-Score*
Random Forest	99,7096	99,8237	**90,9743**	98,1663	94,4336
KNN	98,4946	96,7958	63,7612	92,7058	75,5563
Decision Tree	99,7157	99,1793	90,8408	98,6145	94,5682
XGBoost	**99,7177**	**99,8637**	90,3932	**99,3073**	**94,6408**
Extra Trees	99,6063	99,7572	88,5002	96,903	92,5112



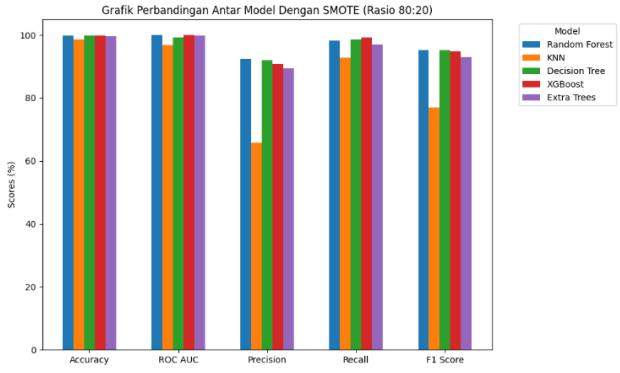
Gambar 8. Grafik Perbandingan Antar Model Dengan *Resampling* SMOTE (Rasio 70:30)

Pada Tabel 5 dan Gambar 8, terlihat bahwa model *XGBoost* masih mendapatkan *accuracy*, *ROC AUC*, *recall*, dan *F1-Score* yang paling baik dibandingkan model lain pada rasio *data train* 70% dan *data test* 30%, sedangkan pada metrik *precision*, model *Random Forest* mendapatkan *score* tertinggi.

b. Rasio 80:20: hasil evaluasi klasifikasi pada data uji dengan rasio pembagian 80:20 dengan teknik *resampling* SMOTE ditampilkan pada Tabel 6 dan Gambar 9.

Tabel 6. Hasil Klasifikasi Dengan *Resampling* SMOTE (Rasio 80:20)

Model	*Accuracy*	*ROC AUC*	*Precision*	*Recall*	*F1-Score*
Random Forest	**99,75**	99,9196	**92,4303**	98,1862	95,2213
KNN	98,5856	96,8806	65,6678	92,7449	76,8922
Decision Tree	**99,75**	99,224	92,0474	98,6699	**95,2437**
XGBoost	99,7254	**99,9589**	90,8135	**99,214**	94,8281
Extra Trees	99,6334	99,8141	89,3712	97,0979	93,0745



Gambar 9. Grafik Perbandingan Antar Model Dengan *Resampling* SMOTE (Rasio 80:20)

Building of Informatics, Technology and Science (BITS)
Volume 6, No 2, Desember 2024 Page: 1427−1439
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i3.6110

Pada rasio data 80:20, Model *Random Forest* dan *Decision Tree* mendapatkan *accuracy* yang sama yaitu 99,75% dan lebih besar dibanding model *XGBoost*. Namun *score ROC AUC* dan *recall* pada *XGBoost* masih mendapatkan hasil yang lebih tinggi dibandingkan model lainnya.

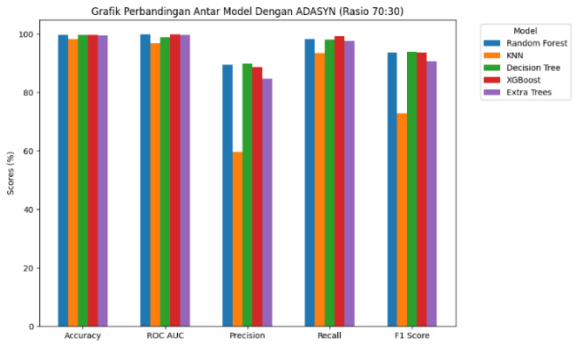
3.3 Hasil Klasifikasi Dengan *Resampling* ADASYN

Dalam tahap pengujian ketiga, pengujian model pembelajaran mesin dilakukan dengan teknik *resampling* ADASYN. Pengujian ini dilakukan dengan dua rasio pembagian data latih dan data uji seperti sebelumnya, yaitu 70:30 dan 80:20.

a. Rasio 70:30: hasil evaluasi klasifikasi pada data uji dengan rasio pembagian 70:30 dengan teknik *resampling* ADASYN ditampilkan pada Tabel 7 dan Gambar 10.

Tabel 7. Hasil Klasifikasi Dengan *Resampling* ADASYN (Rasio 70:30)

Model	*Accuracy*	*ROC AUC*	*Precision*	*Recall*	*F1-Score*
Random Forest	99,6646	**99,7982**	89,3996	98,2885	93,6335
KNN	98,2481	96,8105	59,6259	93,5208	72,8225
Decision Tree	**99,6758**	98,8809	**89,9439**	98,044	**93,8195**
XGBoost	99,6646	99,7935	88,6827	**99,3073**	93,6947
Extra Trees	99,4938	99,7309	84,5747	97,6365	90,6374



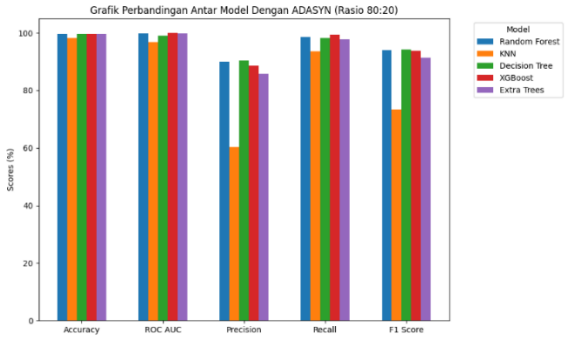
Gambar 10. Grafik Perbandingan Antar Model Dengan *Resampling* ADASYN (Rasio 70:30)

Berbeda dengan *resampling* SMOTE, Model *Decision Tree* justru mendapatkan hasil *accuracy*, *precision*, dan *F1-Score* yang lebih tinggi dibanding model lain nya, namun pada metrik *ROC AUC*, model *Random Forest* yang mendapatkan hasil paling tinggi. Untuk metrik *recall*, model *XGBoost* mendapatkan *score* yang paling tinggi. Meskipun demikian, perbedaan hasil di antara semua model relatif kecil.

b. Rasio 80:20: hasil evaluasi klasifikasi pada data uji dengan rasio pembagian 80:20 dengan teknik *resampling* ADASYN ditampilkan pada Tabel 8 dan Gambar 11.

Tabel 8. Hasil Klasifikasi Dengan *Resampling* ADASYN (Rasio 80:20)

Model	*Accuracy*	*ROC AUC*	*Precision*	*Recall*	*F1-Score*
Random Forest	99,6855	99,9135	89,9614	98,6094	94,0871
KNN	98,2819	96,8488	60,4297	93,5308	73,4219
Decision Tree	**99,6947**	99,019	**90,4841**	98,3071	**94,2336**
XGBoost	99,6656	**99,9692**	88,6853	**99,5163**	93,7892
Extra Trees	99,5352	99,8684	85,7976	97,8839	91,4431



Gambar 11. Grafik Perbandingan Antar Model Dengan *Resampling* ADASYN (Rasio 80:20)

Building of Informatics, Technology and Science (BITS)
Volume 6, No 2, Desember 2024 Page: 1427−1439
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i3.6110

Sama seperti rasio 70:30, *Decision Tree* juga mendapatkan hasil *accuracy*, *Precision*, dan *F1-Score* yang paling tinggi, namun hasil *ROC AUC* dan *recall* pada *XGBoost* masih menjadi yang paling tinggi di antara model lainnya.

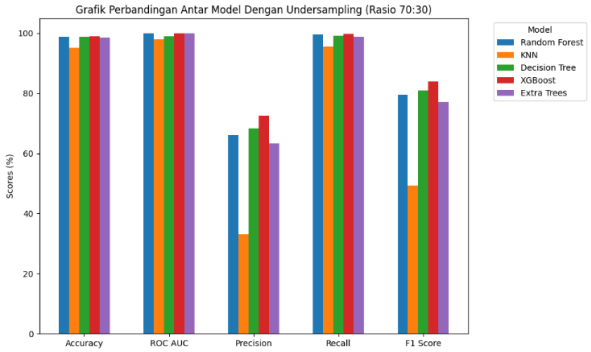
3.4 Hasil Klasifikasi Dengan *Resampling Undersampling*

Pada tahap pengujian keempat, dilakukan evaluasi model pembelajaran mesin dengan menerapkan teknik *resampling Undersampling*. Tidak seperti metode SMOTE dan ADASYN yang menambah data minoritas, teknik *Undersampling* justru mengurangi jumlah data mayoritas untuk mengatasi ketidakseimbangan. Pengujian ini dilakukan dengan dua rasio pembagian data latih dan data uji, yaitu 70:30 dan 80:20, seperti yang telah diterapkan pada tahap sebelumnya.

a. Rasio 70:30: hasil evaluasi klasifikasi pada data uji dengan rasio pembagian 70:30 dengan teknik *resampling Undersampling* ditampilkan pada Tabel 9 dan Gambar 12.

Tabel 9. Hasil Klasifikasi Dengan *Resampling Undersampling* (Rasio 70:30)

Model	*Accuracy*	*ROC AUC*	*Precision*	*Recall*	*F1-Score*
Random Forest	98,7063	99,8881	66,0806	99,5518	79,4342
KNN	95,0562	97,9282	33,1778	95,6398	49,2653
Decision Tree	98,827	98,9418	68,3826	99,0628	80,912
XGBoost	**99,0397**	**99,8941**	**72,4312**	**99,674**	**83,8964**
Extra Trees	98,5283	99,8509	63,261	98,6553	77,0896



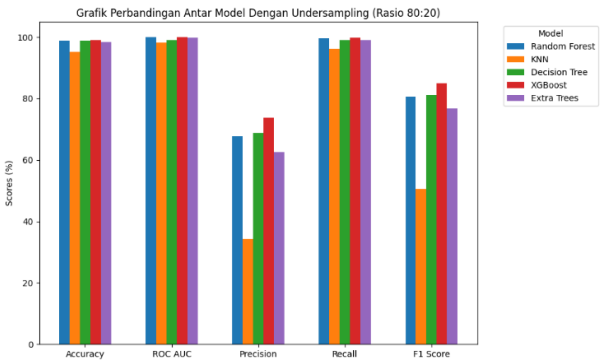
Gambar 12. Grafik Perbandingan Antar Model Dengan *Resampling Undersampling* (Rasio 70:30)

Pada rasio data 70:30 setelah penerapan *undersampling*, Model *XGBoost* mendapatkan *score* paling baik untuk semua metrik baik dari *accuracy*, *ROC AUC*, *Precision*, *Recall*, maupun *F1-Score* dibandingkan model lain.

b. Rasio 80:20: hasil evaluasi klasifikasi pada data uji dengan rasio pembagian 80:20 dengan teknik *resampling Undersampling* ditampilkan pada Tabel 10 dan Gambar 13.

Tabel 10. Hasil Klasifikasi Dengan *Resampling Undersampling* (Rasio 80:20)

Model	*Accuracy*	*ROC AUC*	*Precision*	*Recall*	*F1-Score*
Random Forest	98,7866	99,9382	67,7297	99,6977	80,6554
KNN	95,2291	98,1455	34,3103	96,2515	50,5879
Decision Tree	98,8326	98,93	68,7369	99,0326	81,1494
XGBoost	**99,098**	**99,9578**	**73,8159**	**99,8791**	**84,8921**
Extra Trees	98,4767	99,8896	62,6386	99,0326	76,7393



Gambar 13. Grafik Perbandingan Antar Model Dengan *Resampling Undersampling* (Rasio 80:20)

Building of Informatics, Technology and Science (BITS)
Volume 6, No 2, Desember 2024 Page: 1427−1439
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i3.6110

Pada rasio 80:20 ini, model *XGBoost* juga mendapatkan *score* paling baik dibandingkan model lain untuk semua metrik, yaitu *accuracy*, *ROC AUC*, *Precision*, *Recall*, maupun *F1-Score*.

3.5 Perbandingan Kinerja Model yang Telah Dievaluasi

Pada bagian ini, dilakukan perbandingan kinerja dari berbagai model yang sebelumnya telah dievaluasi dan memiliki *score* tertinggi. Perbandingan ini mencakup performa setiap model yang akan menentukan model terbaik, teknik *resampling* terbaik, dan rasio data terbaik.

3.5.1 Analisis Performa Model

Sebelum dilakukan *resampling*, pada rasio data 70:30 maupun 80:20, model *XGBoost* menunjukkan performa terbaik pada metrik *Accuracy*, *ROC AUC*, *Recall*, dan *F1-Score*, sementara model *Extra Trees* unggul pada metrik *Precision*. Setelah penerapan SMOTE pada rasio data 70:30, model *XGBoost* unggul pada *Accuracy*, *ROC AUC*, *Recall*, dan *F1-Score*, sedangkan *Random Forest* lebih unggul dalam *Precision*. Namun, pada rasio data 80:20, *score Accuracy* tertinggi didapatkan oleh *Random Forest* dan *Decision Tree*, sementara *XGBoost* unggul dalam *ROC AUC* dan *Recall*. Dengan *Resampling* ADASYN pada rasio data 70:30 maupun 80:20, *Decision Tree* memiliki *score Accuracy*, *Precision*, dan *F1-Score* tertinggi, sedangkan *XGBoost* lebih unggul pada *ROC AUC* dan *Recall*. Namun, *score* pada rasio data 80:20, lebih tinggi dibandingkan *score* pada rasio data 70:30 untuk *resampling* ADASYN. Terakhir, dengan *Resampling Undersampling* pada rasio data 70:30 dan 80:20, *XGBoost* memiliki *score* terbaik untuk semua metrik dari *Accuracy*, *ROC AUC*, *Precision*, *Recall*, dan *F1-Score*. Namun *score* dengan rasio data 80:20 lebih tinggi dibandingkan rasio data 70:30 untuk *resampling Undersampling*.

3.5.2 Analisis Performa Berdasarkan Rasio Data

Berdasarkan analisis performa model, rasio data 80:20 menunjukkan *score* yang lebih tinggi dibandingkan rasio 70:30. baik sebelum *resampling* maupun setelah dilakukan *resampling* menggunakan teknik SMOTE, ADASYN, dan *Undersampling*. Hal ini mengindikasikan bahwa rasio 80:20 menghasilkan distribusi data yang lebih optimal untuk pelatihan model, sehingga meningkatkan kemampuan model dalam mendeteksi kelas minoritas maupun mayoritas.

3.5.3 Resampling Terbaik

Berdasarkan hasil evaluasi, teknik *resampling* SMOTE, ADASYN, dan *Undersampling* mempengaruhi performa model yang berbeda. SMOTE meningkatkan performa model, terutama pada model *XGBoost*, dalam hal *Accuracy*, *Recall*, dan *ROC AUC*. Teknik ADASYN memberikan peningkatan pada *Precision* dan *F1-Score* pada model *Decision Tree*. Sementara itu, teknik *Undersampling* menghasilkan performa terbaik untuk model *XGBoost* pada rasio data 80:20 dan 70:30 untuk semua metrik. Secara keseluruhan, SMOTE menjadi teknik yang paling signifikan dalam meningkatkan performa model, terutama pada metrik utama seperti *Accuracy*, *Precision*, dan *F1-Score*.

3.6 Rekapitulasi Kinerja Model

Pada bagian ini menyajikan rekapitulasi kinerja berbagai model yang diuji untuk mendeteksi penipuan transaksi keuangan. Hasil rekapitulasi kinerja model secara rinci dapat dilihat pada Tabel 11.

Tabel 11. Rekapitulasi Kinerja Model yang Telah Dievaluasi

Model	Rasio Data	*Accuracy*	*ROC AUC*	*Precision*	*Recall*	*F1-Score*
Sebelum *Resampling*						
XGBoost	70:30	**99,8251**	99,8743	97,2671	95,7213	96,488
Extra Trees	70:30	99,6032	99,7299	**98,181**	85,7783	91,5615
XGBoost	80:20	**99,8251**	**99,9733**	97,2393	**95,8283**	**96,5286**
Extra Trees	80:20	99,618	99,7901	98,1494	86,578	92,0013
Dengan *Resampling* SMOTE						
Random Forest	70:30	99,7096	99,8237	90,9743	98,1663	94,4336
XGBoost	70:30	99,7177	99,8637	90,3932	**99,3073**	94,6408
Random Forest	80:20	**99,75**	99,9196	**92,4303**	98,1862	95,2213
Decision Tree	80:20	**99,75**	99,224	92,0474	98,6699	**95,2437**
XGBoost	80:20	99,7254	**99,9589**	90,8135	99,214	94,8281
Dengan *Resampling* ADASYN						
Decision Tree	70:30	99,6758	98,8809	89,9439	98,044	93,8195
XGBoost	70:30	99,6646	99,7935	88,6827	99,3073	93,6947
Decision Tree	80:20	**99,6947**	99,019	**90,4841**	98,3071	**94,2336**
XGBoost	80:20	99,6656	**99,9692**	88,6853	**99,5163**	93,7892
Dengan *Resampling Undersampling*						
XGBoost	70:30	99,0397	99,8941	72,4312	99,674	83,8964
XGBoost	80:20	**99,098**	**99,9578**	**73,8159**	**99,8791**	**84,8921**

Building of Informatics, Technology and Science (BITS)
Volume 6, No 2, Desember 2024 Page: 1427−1439
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i3.6110

Secara keseluruhan, teknik resampling *SMOTE* dan *Undersampling* terbukti meningkatkan performa model dalam mendeteksi penipuan pada data yang tidak seimbang. Di sisi lain, teknik *Undersampling* juga menunjukkan pengaruh yang positif, terutama pada model ***XGBoost***, yang menunjukkan skor tertinggi pada semua metrik saat digunakan dengan rasio data 80:20. Secara keseluruhan, ***XGBoost*** secara konsisten menghasilkan skor tertinggi pada berbagai metrik utama, yang menunjukkan bahwa model ini paling mampu memanfaatkan kelebihan dari teknik *resampling*.

4. KESIMPULAN

Penelitian ini telah mengevaluasi performa beberapa model pembelajaran mesin, yaitu *Random Forest*, *K-Nearest Neighbors* (KNN), *Decision Tree*, *XGBoost*, dan *Extra Trees*, dalam mendeteksi penipuan pada transaksi keuangan. Penilaian dilakukan dengan membandingkan performa model sebelum dan sesudah penerapan teknik *resampling* untuk mengatasi ketidakseimbangan data, yaitu SMOTE, ADASYN, dan *Undersampling*. Selain itu, dua rasio pembagian data latih dan data uji, yaitu 70:30 dan 80:20, digunakan untuk menilai efektivitas model pada berbagai kondisi data. Berdasarkan hasil evaluasi, ***XGBoost*** terbukti sebagai model dengan performa paling konsisten, terutama setelah *resampling undersampling*. Di antara teknik resampling yang digunakan, SMOTE dan *Undersampling* menunjukkan hasil yang signifikan dalam meningkatkan performa model. SMOTE lebih unggul dalam meningkatkan *ROC AUC* dan *Recall* pada model ***XGBoost***, sementara *Undersampling* juga memberikan hasil terbaik pada ***XGBoost*** untuk semua metrik, terutama pada rasio 80:20. Dari analisis rasio data, rasio 80:20 menunjukkan distribusi yang lebih optimal dibandingkan rasio 70:30, karena memberikan performa model yang lebih tinggi pada berbagai metrik. Hal ini menunjukkan bahwa pembagian data yang lebih besar untuk pelatihan dapat membantu model lebih baik dalam mendeteksi kelas minoritas. Secara keseluruhan, SMOTE dan *Undersampling* adalah teknik *resampling* terbaik dalam penelitian ini, dan ***XGBoost*** menjadi model yang paling efektif dalam mendeteksi penipuan pada transaksi keuangan dengan data tidak seimbang. Hasil dari penelitian ini diharapkan dapat menjadi referensi penting dalam pengembangan metode deteksi penipuan di masa mendatang.

REFERENCES

[1] H. Sun, J. Li, and X. Zhu, “Financial fraud detection based on the part-of-speech features of textual risk disclosures in financial reports,” *Procedia Comput Sci*, vol. 221, pp. 57–64, 2023, Accessed: Oct. 14, 2024. [Online]. Available: https://doi.org/10.1016/j.procs.2023.07.009

[2] S. Wen, J. Li, X. Zhu, and M. Liu, “Analysis of financial fraud based on manager knowledge graph,” *Procedia Comput Sci*, vol. 199, pp. 773–779, 2022, doi: https://doi.org/10.1016/j.procs.2022.01.096.

[3] Z. Zhao and T. Bai, “Financial Fraud Detection and Prediction in Listed Companies Using SMOTE and Machine Learning Algorithms,” *Entropy*, vol. 24, no. 8, p. 1157, 2022, Accessed: Oct. 14, 2024. [Online]. Available: https://www.mdpi.com/1099-4300/24/8/1157

[4] T. Xu, G. Coco, and M. Neale, “A predictive model of recreational water quality based on adaptive synthetic sampling algorithms and machine learning,” *Water Res*, vol. 177, p. 115788, 2020, doi: https://doi.org/10.1016/j.watres.2020.115788.

[5] Q. Zhou and B. Sun, “Adaptive K-means clustering based under-sampling methods to solve the class imbalance problem,” *Data Inf Manag*, vol. 8, no. 3, p. 100064, 2024, doi: https://doi.org/10.1016/j.dim.2023.100064.

[6] J. Bai, Y. Li, J. Li, X. Yang, Y. Jiang, and S.-T. Xia, “Multinomial random forest,” *Pattern Recognit*, vol. 122, p. 108331, 2022, doi: https://doi.org/10.1016/j.patcog.2021.108331.

[7] S. Zhang, “Cost-sensitive KNN classification,” *Neurocomputing*, vol. 391, pp. 234–242, 2020, doi: https://doi.org/10.1016/j.neucom.2018.11.101.

[8] M. M. Ghiasi and S. Zendehboudi, “Application of decision tree-based ensemble learning in the classification of breast cancer,” *Comput Biol Med*, vol. 128, p. 104089, 2021, doi: https://doi.org/10.1016/j.compbiomed.2020.104089.

[9] M. Amjad, I. Ahmad, M. Ahmad, P. Wróblewski, P. Kamiński, and U. Amjad, “Prediction of pile bearing capacity using XGBoost algorithm: modeling and performance evaluation,” *Applied Sciences*, vol. 12, no. 4, p. 2126, 2022, Accessed: Oct. 14, 2024. [Online]. Available: https://www.mdpi.com/2076-3417/12/4/2126

[10] U. Saeed, S. U. Jan, Y.-D. Lee, and I. Koo, “Fault diagnosis based on extremely randomized trees in wireless sensor networks,” *Reliab Eng Syst Saf*, vol. 205, p. 107284, 2021, doi: https://doi.org/10.1016/j.ress.2020.107284.

[11] F. Zamachsari and N. Puspitasari, “Penerapan Deep Learning dalam Deteksi Penipuan Transaksi Keuangan Secara Elektronik,” *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 5, no. 2, pp. 203–212, 2021, Accessed: Oct. 15, 2024. [Online]. Available: https://jurnal.iaii.or.id/index.php/RESTI/article/view/2952/391

[12] L. Hasibuan and F. Jannah, “Deteksi Penipuan Kartu Kredit Menggunakan Support Vector Machine dengan Optimasi Grid Search dan Genetic Algorithm,” *Building of Informatics, Technology and Science (BITS)*, vol. 6, no. 1, Jun. 2024, doi: 10.47065/bits.v6i1.5355.

[13] M. Febriady, S. Samsuryadi, and D. P. Rini, “Klasifikasi Transaksi Penipuan Pada Kartu Kredit Menggunakan Metode Resampling Dan Pembelajaran Mesin,” *JURNAL MEDIA INFORMATIKA BUDIDARMA*, vol. 6, no. 2, pp. 1010–1016, 2022, Accessed: Oct. 15, 2024. [Online]. Available: https://ejurnal.stmik-budidarma.ac.id/index.php/mib/article/view/3515/2649

[14] W. Priatna, “Dampak Pengambilan Sampel Data untuk Optimalisasi Data tidak seimbang pada Klasifikasi Penipuan Transaksi E-Commerce,” *Indonesian Journal of Computer Science*, vol. 13, no. 2, 2024, Accessed: Oct. 15, 2024. [Online]. Available: http://ijcs.net/ijcs/index.php/ijcs/article/view/3698

Building of Informatics, Technology and Science (BITS)
Volume 6, No 2, Desember 2024 Page: 1427−1439
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v6i3.6110

[15] K. Kurniabudi, A. Harris, and V. Veronica, "Komparasi Performa Tree-Based Classifier Untuk Deteksi Anomali Pada Data Berdimensi Tinggi dan Tidak Seimbang," *Jurnal Media Informatika Budidarma*, vol. 6, no. 1, pp. 370–377, 2022, Accessed: Oct. 15, 2024. [Online]. Available: https://www.ejurnal.stmik-budidarma.ac.id/index.php/mib/article/view/3473/2431

[16] W. Liang, S. Luo, G. Zhao, and H. Wu, "Predicting hard rock pillar stability using GBDT, XGBoost, and LightGBM algorithms," *Mathematics*, vol. 8, no. 5, p. 765, 2020, Accessed: Oct. 19, 2024. [Online]. Available: https://www.mdpi.com/2227-7390/8/5/765

[17] A. Ramadina and K. D. Tania, "Knowledge Extraction of Gojek Application Review Using Aspect-based Sentiment Analysis," *The Indonesian Journal of Computer Science*, vol. 13, no. 3, 2024, Accessed: Oct. 19, 2024. [Online]. Available: https://ejurnal.seminar-id.com/index.php/bits/article/view/5368/2982

[18] L. Camacho, G. Douzas, and F. Bacao, "Geometric SMOTE for regression," *Expert Syst Appl*, vol. 193, p. 116387, 2022, doi: https://doi.org/10.1016/j.eswa.2021.116387.

[19] G. Ahmed *et al.*, "Dad-net: Classification of alzheimer's disease using adasyn oversampling technique and optimized neural network," *Molecules*, vol. 27, no. 20, p. 7085, 2022, Accessed: Oct. 16, 2024. [Online]. Available: https://www.mdpi.com/1420-3049/27/20/7085

[20] Q. Dai, J. Liu, and Y. Liu, "Multi-granularity relabeled under-sampling algorithm for imbalanced data," *Appl Soft Comput*, vol. 124, p. 109083, 2022, doi: https://doi.org/10.1016/j.asoc.2022.109083.

[21] J. Li, C. Guo, S. Lv, Q. Xie, and X. Zheng, "Financial fraud detection for Chinese listed firms: Does managers' abnormal tone matter?," *Emerging Markets Review*, vol. 62, p. 101170, 2024, doi: https://doi.org/10.1016/j.ememar.2024.101170.

[22] A. Shokrzade, M. Ramezani, F. Akhlaghian Tab, and M. Abdulla Mohammad, "A novel extreme learning machine based kNN classification method for dealing with big data," *Expert Syst Appl*, vol. 183, p. 115293, 2021, doi: https://doi.org/10.1016/j.eswa.2021.115293.

[23] B. Charbuty and A. Abdulazeez, "Classification based on decision tree algorithm for machine learning," *Journal of Applied Science and Technology Trends*, vol. 2, no. 01, pp. 20–28, 2021, Accessed: Oct. 14, 2024. [Online]. Available: https://www.jastt.org/index.php/jasttpath/article/view/65/24

[24] A. Izotova and A. Valiullin, "Comparison of Poisson process and machine learning algorithms approach for credit card fraud detection," *Procedia Comput Sci*, vol. 186, pp. 721–726, 2021, doi: https://doi.org/10.1016/j.procs.2021.04.214.

[25] M. Seyyedattar, M. M. Ghiasi, S. Zendehboudi, and S. Butt, "Determination of bubble point pressure and oil formation volume factor: Extra trees compared with LSSVM-CSA hybrid and ANFIS models," *Fuel*, vol. 269, p. 116834, 2020, doi: https://doi.org/10.1016/j.fuel.2019.116834.

[26] X. Deng, H. Shao, L. Shi, X. Wang, and T. Xie, "A classification–detection approach of COVID-19 based on chest X-ray and CT by using keras pre-trained deep learning models," *Computer Modeling in Engineering & Sciences*, vol. 125, no. 2, pp. 579–596, 2020, Accessed: Oct. 16, 2024. [Online]. Available: https://www.ingentaconnect.com/contentone/tsp/cmes/2020/00000125/00000002/art00006#