

# Deteksi Kecurangan Transaksi Menggunakan Random Forest Classification untuk Analisis Transaksi Online

*Online Transaction Fraud Detection Using Random Forest Classification*

**Parulian Pangaribuan<sup>a,1</sup>, Budi Triandi<sup>b,2</sup>, Ratih Puspa Sari<sup>c,3</sup>**

<sup>a</sup>Program Studi Informatika, Fakultas Teknik dan Ilmu Komputer, Universitas Potensi Utama, Medan, Indonesia.

<sup>b</sup> Program Studi Ilmu Komputer, Fakultas Teknik dan Ilmu Komputer, Universitas Potensi Utama, Medan, Indonesia

<sup>c</sup>Program Studi Sistem Informasi, Fakultas Teknik dan Ilmu Komputer, Universitas Potensi Utama, Medan, Indonesia

parulianpangaribuan@gmail.com<sup>1</sup>, buditriandi@gmail.com<sup>2</sup>, puspasariratih21@gmail.com<sup>3</sup>

---

## ABSTRAK

Pertumbuhan transaksi digital meningkatkan peluang terjadinya kecurangan transaksi, sehingga diperlukan model deteksi yang mampu bekerja cepat, akurat, dan dapat dijelaskan. Penelitian ini bertujuan menerapkan algoritma Random Forest Classification untuk mendeteksi kecurangan transaksi online berdasarkan data transaksi sekunder. Data yang digunakan adalah Credit Card Fraud Dataset yang memuat fitur jarak transaksi, rasio harga transaksi terhadap median pembelian, penggunaan chip, penggunaan PIN, transaksi online, dan label fraud. Tahapan penelitian mencakup pemahaman masalah, data overview, exploratory data analysis, pembersihan data, penanganan outlier, pembagian data 80:20, pelatihan Random Forest Classifier, evaluasi model, serta analisis feature importance. Rumus yang digunakan meliputi voting mayoritas Random Forest, Gini Index, penurunan impurity, accuracy, precision, recall, F1-score, TPR, FPR, AUC, dan feature importance. Hasil penelitian menunjukkan akurasi sebesar 98% dengan AUC 0,87. Model sangat baik mengenali transaksi tidak curang dengan precision 97% dan recall 100%, tetapi recall pada kelas curang masih 72% karena terdapat 4.870 false negative. Fitur `ratio_to_median_purchase_price` menjadi variabel paling dominan, diikuti `online_order` dan `repeat_retailer`. Hasil ini menunjukkan bahwa Random Forest berpotensi menjadi alat bantu deteksi kecurangan transaksi online, meskipun peningkatan recall kelas fraud tetap perlu dilakukan.

Kata Kunci : deteksi kecurangan, Random Forest, transaksi online, klasifikasi, ketidakseimbangan data.

## ABSTRACT

The rapid growth of digital transactions increases the risk of transaction fraud and requires a detection model that is fast, accurate, and explainable. This study implements the Random Forest Classification algorithm to detect online transaction fraud using a secondary transaction dataset. The study uses the Credit Card Fraud Dataset, which contains transaction distance, transaction-to-median price ratio, chip usage, PIN usage, online transaction status, and fraud label. The research stages include problem understanding, data overview, exploratory data analysis, data cleaning, outlier handling, 80:20 train-test split, Random Forest Classifier training, model evaluation, and feature importance analysis. The complete formulas include Random Forest majority voting, Gini Index, impurity reduction, accuracy, precision, recall, F1-score, TPR, FPR, AUC, and feature importance. The results show an accuracy of 98% and an AUC of 0.87. The model identifies legitimate transactions very well, with 97% precision and 100% recall, but the recall for fraudulent transactions remains 72% because 4,870 false negatives are still found. The most dominant feature is `ratio_to_median_purchase_price`, followed by `online_order` and `repeat_retailer`. These findings indicate that Random Forest has potential as a decision-support tool for online transaction fraud detection, although recall improvement for the fraud class remains necessary.

Keywords : fraud detection, Random Forest, online transactions, classification, class imbalance.

---

Info Artikel :

Disubmit:

Direview:

Diterima :

Copyright © 2026 - Journal UPU. All rights reserved.

---

DOI: <https://www.doi.org/10.22303/upu.1.1.2021.01-10>

## 1. PENDAHULUAN

Transaksi *online* berkembang sangat cepat melalui *e-commerce*, perbankan digital, dompet elektronik, dan layanan pembayaran berbasis aplikasi. Perubahan ini memudahkan pengguna, tetapi juga membuka peluang kecurangan transaksi. Bentuk kecurangan dapat muncul melalui penyalahgunaan identitas, transaksi tidak wajar, manipulasi sistem pembayaran, penggunaan data kartu secara ilegal, dan pola transaksi yang tidak sesuai dengan kebiasaan pengguna [1], [10], [14].

Deteksi kecurangan tidak mudah dilakukan secara manual karena volume data transaksi sangat besar dan pola kecurangan sering tersembunyi. Sistem berbasis aturan tetap berguna, tetapi aturan statis sulit mengikuti perubahan perilaku pelaku *fraud*. Oleh karena itu, pendekatan *machine learning* menjadi relevan karena dapat mempelajari pola historis dan membedakan transaksi normal dengan transaksi mencurigakan secara lebih adaptif [1], [7], [12].

Salah satu masalah utama dalam deteksi *fraud* adalah ketidakseimbangan kelas. Pada data transaksi, jumlah transaksi tidak curang jauh lebih besar dibandingkan transaksi curang. Dataset dalam penelitian ini menunjukkan 912.597 transaksi tidak curang atau 91,26%, sedangkan transaksi curang berjumlah 87.403 data atau 8,74%. Kondisi ini dapat membuat model cenderung mengenali kelas mayoritas dan kurang sensitif terhadap kelas *fraud* [2], [6], [8].

*Random Forest* dipilih sebagai metode utama karena algoritma ini membangun banyak pohon keputusan dan menggabungkan hasilnya melalui voting. Pendekatan *ensemble* tersebut dapat mengurangi varians, menangani hubungan antar fitur yang kompleks, dan memberikan informasi *feature importance* untuk membantu interpretasi model. Dalam konteks *fraud detection*, kemampuan ini penting karena pengambil keputusan tidak hanya membutuhkan prediksi, tetapi juga alasan teknis yang mendasari prediksi tersebut [2], [4], [13].

Penelitian ini berangkat dari kebutuhan membangun model klasifikasi yang mampu mendeteksi transaksi curang dengan akurasi tinggi dan tetap memperhatikan kelas minoritas. Fokus penelitian diarahkan pada penerapan *Random Forest Classification*, evaluasi kinerja model melalui *accuracy*, *precision*, *recall*, *F1-score*, *confusion matrix*, *ROC Curve*, dan *AUC*, serta analisis *feature importance* untuk mengetahui fitur yang paling berpengaruh dalam prediksi.

Kontribusi artikel ini terletak pada penyusunan alur kerja deteksi kecurangan transaksi *online* secara runtut, mulai dari data *overview*, eksplorasi awal, preprocessing, pemodelan *Random Forest*, evaluasi multi-metrik, hingga interpretasi fitur. Artikel ini juga menekankan bahwa model dengan akurasi tinggi tetap perlu dikritisi melalui *recall* kelas *fraud* dan jumlah *false negative*, karena kesalahan tersebut dapat menyebabkan transaksi curang tidak terdeteksi.

### A. Posisi Penelitian terhadap Studi Terkait

Penelitian terdahulu menunjukkan bahwa deteksi kecurangan transaksi dapat dilakukan dengan berbagai pendekatan *machine learning*. Beberapa studi menggunakan *Random Forest*, *Gradient Boosting*, *SMOTE*, dan model *hybrid* untuk meningkatkan sensitivitas terhadap transaksi curang. Posisi penelitian ini berada pada penerapan *Random Forest* sebagai model utama dengan penekanan pada evaluasi multi-metrik dan interpretasi *feature importance*. Ringkasan posisi penelitian disajikan pada Tabel 1.

Tabel 1. Posisi Penelitian terhadap Studi Terkait

| Penelitian | Fokus | Relevansi |
|------------|-------|-----------|
|------------|-------|-----------|

|                          |                                                                                     |                                                                                             |
|--------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Almazroi dan Ayub [1]    | Model <i>online payment fraud</i> detection berbasis <i>machine learning</i> .      | Menjadi dasar bahwa <i>machine learning</i> relevan untuk sistem pembayaran <i>online</i> . |
| Aburbeian dan Ashqar [2] | Enhanced <i>Random Forest</i> untuk data kartu kredit tidak seimbang.               | Menegaskan pentingnya penanganan <i>imbalanced data</i> dalam <i>fraud detection</i> .      |
| Du dan Zhai [4]          | <i>Random Forest</i> pada financial recognition model.                              | Mendukung penggunaan <i>Random Forest</i> untuk pola transaksi kompleks.                    |
| Ilham et al. [6]         | <i>SMOTE-Tomek</i> dan <i>Random Forest</i> pada data transaksi <i>fraud</i> .      | Menunjukkan bahwa resampling dapat meningkatkan deteksi kelas minoritas.                    |
| Rafid [12]               | Implementasi <i>Random Forest</i> untuk <i>online transaction fraud detection</i> . | Relevan dengan fokus transaksi <i>online</i> dan pemodelan berbasis fitur.                  |
| Pratama dan Wahid [11]   | <i>Random Forest</i> dan <i>Gradient Boosting</i> pada sistem <i>online</i> .       | Menjadi rujukan untuk pengembangan model <i>ensemble</i> lebih lanjut.                      |

## 2. METODE

### A. Desain Penelitian dan Sumber Data

Penelitian ini menggunakan pendekatan kuantitatif komputasional dengan metode *machine learning*. Data yang digunakan bersifat sekunder karena diperoleh dari *dataset* publik dan tidak dikumpulkan langsung dari responden. Seluruh proses penelitian dilakukan melalui perangkat lunak *Python* dengan pustaka pendukung seperti *Pandas*, *NumPy*, *Matplotlib*, dan *Scikit-learn*.

Objek penelitian berupa data transaksi dengan label biner, yaitu kelas 0 untuk transaksi tidak curang dan kelas 1 untuk transaksi curang. Dataset berisi tujuh fitur prediktor dan satu label target. Fitur tersebut mencakup *distance\_from\_home*, *distance\_from\_last\_transaction*, *ratio\_to\_median\_purchase\_price*, *repeat\_retailer*, *used\_chip*, *used\_pin\_number*, dan *online\_order*. Label *fraud* digunakan sebagai variabel dependen yang menjadi target klasifikasi.

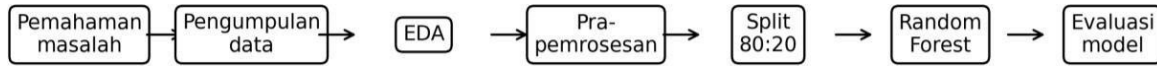
Dataset dibagi menjadi data latih dan data uji dengan proporsi 80:20. Hasil pembagian menunjukkan *X\_train* sebanyak 800.000 sampel dengan 7 fitur, *X\_test* sebanyak 200.000 sampel dengan 7 fitur, *y\_train* sebanyak 800.000 label, dan *y\_test* sebanyak 200.000 label. Pembagian ini digunakan untuk menguji kemampuan model pada data yang belum pernah dilihat selama pelatihan.

Tabel 2. Deskripsi Fitur Dataset Transaksi

| No | Fitur                                 | Keterangan                                                   |
|----|---------------------------------------|--------------------------------------------------------------|
| 1  | <i>distance_from_home</i>             | Jarak lokasi transaksi dari rumah pengguna.                  |
| 2  | <i>distance_from_last_transaction</i> | Jarak lokasi transaksi saat ini dari transaksi sebelumnya.   |
| 3  | <i>ratio_to_median_purchase_price</i> | Rasio nilai transaksi terhadap harga median pembelian.       |
| 4  | <i>repeat_retailer</i>                | Indikator transaksi pada retailer yang sama.                 |
| 5  | <i>used_chip</i>                      | Indikator penggunaan chip kartu.                             |
| 6  | <i>used_pin_number</i>                | Indikator penggunaan PIN dalam transaksi.                    |
| 7  | <i>online_order</i>                   | Indikator transaksi dilakukan secara <i>online</i> .         |
| 8  | <i>fraud</i>                          | Label target, yaitu 0 untuk tidak curang dan 1 untuk curang. |

### B. Tahapan Penelitian

Tahapan penelitian disusun untuk memastikan model dibangun melalui proses yang dapat ditelusuri dan direplikasi. Proses dimulai dari pemahaman masalah, pengumpulan *dataset*, eksplorasi data, pembersihan data, penanganan outlier, analisis distribusi kelas, pembagian data, pelatihan model *Random Forest*, evaluasi kinerja, dan interpretasi *feature importance*.



Gambar 1. Alur penelitian deteksi kecurangan transaksi berbasis Random Forest

Tabel 3. Ringkasan Tahapan Penelitian

| No | Tahap                            | Uraian                                                                                                                                  |
|----|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Problem understanding            | Menentukan masalah utama berupa deteksi transaksi curang pada data <i>online</i> .                                                      |
| 2  | Data overview                    | Memeriksa jumlah data, fitur, tipe data, label, dan struktur <i>dataset</i> .                                                           |
| 3  | <i>Exploratory Data Analysis</i> | Menganalisis distribusi fitur dan pola awal antar kelas.                                                                                |
| 4  | Data cleaning and preprocessing  | Membersihkan data, memeriksa duplikasi, dan menangani outlier.                                                                          |
| 5  | Train-test split                 | Membagi data menjadi 80% pelatihan dan 20% pengujian.                                                                                   |
| 6  | Model training                   | Melatih <i>Random Forest Classifier</i> dengan data latih.                                                                              |
| 7  | Model evaluation                 | Mengukur <i>accuracy</i> , <i>precision</i> , <i>recall</i> , <i>F1-score</i> , <i>confusion matrix</i> , <i>ROC</i> , dan <i>AUC</i> . |
| 8  | Interpretability analysis        | Menganalisis <i>feature importance</i> untuk melihat kontribusi tiap fitur.                                                             |

### C. Rumus Random Forest dan Evaluasi Model

*Random Forest* membentuk banyak pohon keputusan dari sampel *bootstrap*. Setiap pohon menghasilkan prediksi, lalu prediksi akhir diperoleh melalui voting mayoritas. Rumus berikut digunakan untuk menjelaskan proses pembentukan model, pemilihan split berbasis Gini, serta evaluasi hasil klasifikasi.

$$D_b = \{(x_i, y_i)\}_{i=1}^{n_b}, \quad b = 1, 2, \dots, B \quad (1)$$

$$h_b(x) = \text{Tree}_b(x) \quad (2)$$

$$\hat{y}(x) = \text{mode}\{h_1(x), h_2(x), \dots, h_B(x)\} \quad (3)$$

$$\text{Gini}(t) = 1 - \sum_{k=1}^K p_{k,t}^2 \quad (4)$$

$$\Delta \text{Gini}(s, t) = \text{Gini}(t) - \frac{N_L}{N_t} \text{Gini}(t_L) - \frac{N_R}{N_t} \text{Gini}(t_R) \quad (5)$$

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \quad (6)$$

$$\text{Precision} = \frac{TP}{TP + FP} \quad (7)$$

$$\text{Recall} = \frac{TP}{TP + FN} \quad (8)$$

$$F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (9)$$

$$\text{TPR} = \frac{TP}{TP + FN}, \quad \text{FPR} = \frac{FP}{FP + TN} \quad (10)$$

$$\text{AUC} = \int_0^1 \text{TPR}(\text{FPR}) d\text{FPR} \quad (11)$$

$$FI_j = \frac{1}{B} \sum_{b=1}^B \sum_{t \in T_b: v(t)=j} \frac{N_t}{N} \Delta \text{Gini}(t) \quad (12)$$

Rumus (1)-(12). Rumus Random Forest dan metrik evaluasi model

Keterangan:  $D_b$  adalah data *bootstrap* ke- $b$ ,  $h_b(x)$  adalah prediksi pohon ke- $b$ ,  $B$  adalah jumlah pohon,  $p_{\{k,t\}}$  adalah proporsi kelas  $k$  pada node  $t$ ,  $N_L$  dan  $N_R$  adalah jumlah sampel pada cabang kiri dan kanan,  $TP$  adalah *true positive*,  $TN$  adalah *true negative*,  $FP$  adalah *false positive*,  $FN$  adalah *false negative*,  $TPR$  adalah *true positive rate*,  $FPR$  adalah *false positive rate*, dan  $FI_j$  adalah *feature importance* untuk fitur ke- $j$ .

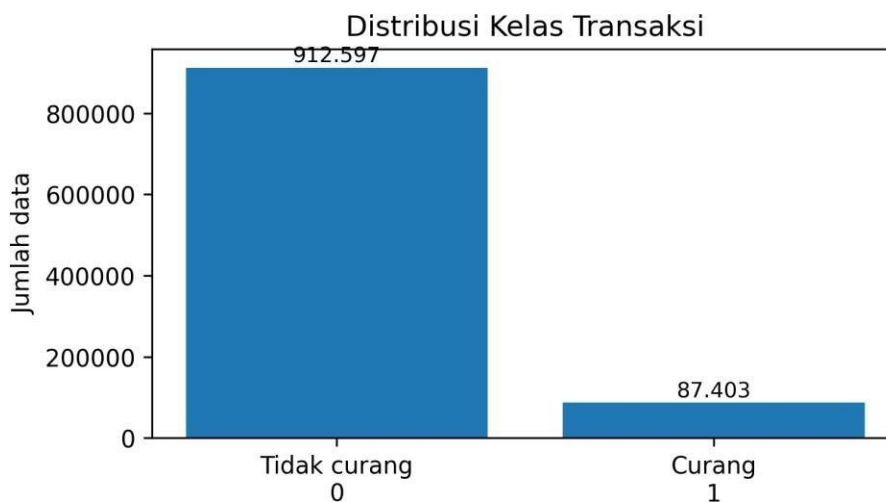
Tabel 4. Parameter dan Komponen Utama Model

| Komponen         | Nilai atau Fungsi                                                                           |
|------------------|---------------------------------------------------------------------------------------------|
| Algoritma        | <i>Random Forest Classifier</i> untuk klasifikasi biner <i>fraud</i> dan <i>non-fraud</i> . |
| Data latih       | 800.000 sampel atau 80% dari total data.                                                    |
| Data uji         | 200.000 sampel atau 20% dari total data.                                                    |
| Jumlah fitur     | 7 fitur prediktor dan 1 label target.                                                       |
| Penanganan kelas | Menggunakan <i>class_weight = balanced</i> untuk membantu kelas minoritas.                  |
| Metrik evaluasi  | <i>Accuracy, precision, recall, F1-score, confusion matrix, ROC Curve, AUC</i> .            |

### 3. HASIL DAN PEMBAHASAN

#### A. Karakteristik Dataset dan Ketidakseimbangan Kelas

Dataset transaksi menunjukkan distribusi kelas yang tidak seimbang. Transaksi tidak curang berjumlah 912.597 data atau 91,26%, sedangkan transaksi curang berjumlah 87.403 data atau 8,74%. Ketidakseimbangan ini menjadi tantangan penting karena model dapat menghasilkan akurasi tinggi hanya dengan mengenali kelas mayoritas. Oleh karena itu, penelitian tidak hanya menilai *accuracy*, tetapi juga *precision*, *recall*, *F1-score*, *confusion matrix*, dan *AUC*.



Gambar 2. Distribusi kelas transaksi pada dataset

Tabel 5. Distribusi Kelas Transaksi

| Kelas | Jumlah Data | Persentase | Makna                   |
|-------|-------------|------------|-------------------------|
| 0     | 912.597     | 91,26%     | Transaksi tidak curang. |
| 1     | 87.403      | 8,74%      | Transaksi curang.       |
| Total | 1.000.000   | 100%       | Seluruh data transaksi. |

#### B. Hasil Pra-pemrosesan Data

Tahap pra-pemrosesan dilakukan untuk memastikan data siap digunakan pada model. Proses ini mencakup pemeriksaan struktur *dataset*, pengecekan missing values, pengecekan duplikasi, identifikasi outlier, dan pemisahan fitur dengan label. Fitur dengan nilai ekstrem diperiksa karena transaksi *fraud* sering muncul sebagai anomali, terutama pada jarak transaksi dan rasio harga transaksi terhadap median pembelian.

Penanganan outlier dilakukan secara hati-hati. Pada kasus *fraud detection*, nilai ekstrem tidak selalu berarti kesalahan data karena dapat menjadi sinyal transaksi mencurigakan. Oleh sebab itu, pembersihan data tidak diarahkan untuk menghapus semua nilai ekstrem, tetapi memastikan bahwa data yang digunakan tidak mengandung nilai tidak valid yang mengganggu proses pelatihan.

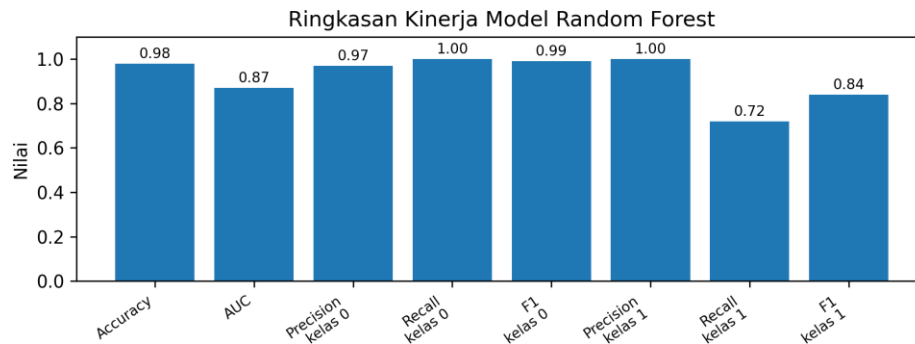
### C. Pembentukan Model Random Forest

Model *Random Forest* dilatih menggunakan data latih berjumlah 800.000 sampel. Setiap decision tree dalam model mempelajari pola dari subset data dan subset fitur. Hasil akhir ditentukan melalui voting mayoritas dari seluruh pohon. Pendekatan ini membuat model lebih stabil dibandingkan decision tree tunggal karena kesalahan dari satu pohon dapat dikompensasi oleh pohon lain.

Penggunaan *class\_weight* = balanced membantu model memberikan perhatian lebih pada kelas minoritas. Strategi ini penting karena kelas *fraud* memiliki jumlah lebih kecil. Tanpa penyesuaian bobot, model dapat lebih banyak mengutamakan prediksi kelas tidak curang sehingga *recall* kelas *fraud* menjadi rendah.

### D. Evaluasi Kinerja Model

Hasil evaluasi menunjukkan bahwa model mencapai *accuracy* sebesar 98% dan *AUC* sebesar 0,87. Nilai ini menunjukkan bahwa *Random Forest* memiliki kemampuan yang baik dalam membedakan transaksi curang dan tidak curang. Namun, hasil *classification report* memperlihatkan perbedaan performa antar kelas, terutama pada *recall* kelas *fraud*.



Gambar 3. Ringkasan kinerja model Random Forest

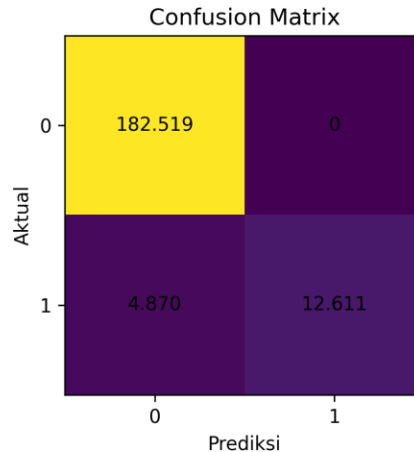
Tabel 6. Classification Report Model Random Forest

| Kelas            | Precision | Recall | F1-score | Interpretasi                                                                       |
|------------------|-----------|--------|----------|------------------------------------------------------------------------------------|
| 0.0 Tidak curang | 0,97      | 1,00   | 0,99     | Model sangat kuat mengenali transaksi tidak curang.                                |
| 1.0 Curang       | 1,00      | 0,72   | 0,84     | Prediksi <i>fraud</i> sangat tepat, tetapi sebagian <i>fraud</i> belum terdeteksi. |
| Accuracy         | -         | -      | 0,98     | Sebanyak 98% data uji diklasifikasikan dengan benar.                               |
| Macro average    | 0,99      | 0,86   | -        | Rata-rata sederhana dari kedua kelas.                                              |
| Weighted average | 0,98      | 0,98   | -        | Rata-rata dengan mempertimbangkan proporsi kelas.                                  |

Pada kelas 0.0 atau transaksi tidak curang, *precision* sebesar 97% dan *recall* sebesar 100% menunjukkan bahwa hampir seluruh transaksi tidak curang dapat dikenali dengan benar. Pada kelas 1.0 atau transaksi curang, *precision* sebesar 100% menunjukkan bahwa prediksi *fraud* yang diberikan model sangat tepat. Namun, *recall* sebesar 72% menunjukkan bahwa masih ada transaksi curang yang diprediksi sebagai tidak curang.

## E. Analisis Confusion Matrix

Confusion matrix memberi gambaran lebih rinci mengenai kesalahan model. Dari 200.000 data uji, model menghasilkan 182.519 *true negative*, 12.611 *true positive*, 0 *false positive*, dan 4.870 *false negative*. Nilai *false negative* menjadi catatan penting karena menunjukkan transaksi yang sebenarnya curang tetapi diprediksi tidak curang.



Gambar 4. Confusion matrix model Random Forest

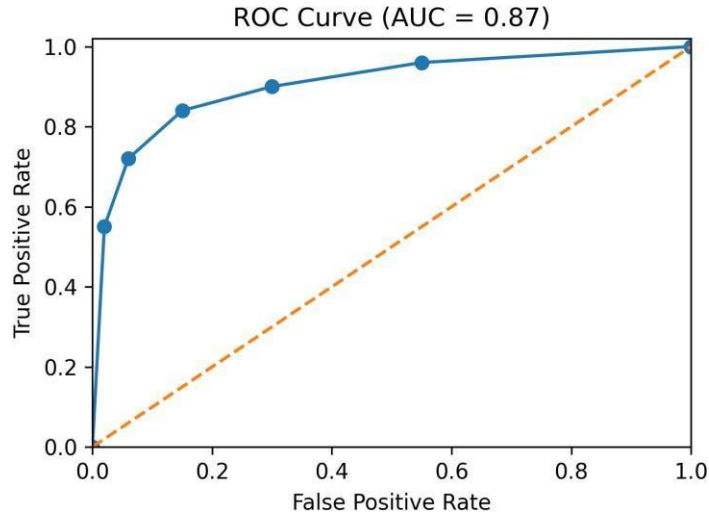
Tabel 7. Confusion Matrix Model Random Forest

| Label Aktual | Prediksi 0 | Prediksi 1 | Total   |
|--------------|------------|------------|---------|
| Aktual 0     | 182.519    | 0          | 182.519 |
| Aktual 1     | 4.870      | 12.611     | 17.481  |
| Total        | 187.389    | 12.611     | 200.000 |

Tidak adanya *false positive* menunjukkan bahwa model tidak salah menandai transaksi normal sebagai *fraud* pada data uji. Kondisi ini baik dari sisi efisiensi karena dapat mengurangi beban pemeriksaan manual. Namun, jumlah *false negative* sebanyak 4.870 perlu menjadi perhatian karena dalam sistem keamanan transaksi, transaksi curang yang lolos deteksi dapat menyebabkan kerugian finansial. Dengan demikian, pengembangan berikutnya perlu diarahkan pada peningkatan *recall* kelas *fraud*.

## F. ROC Curve dan AUC

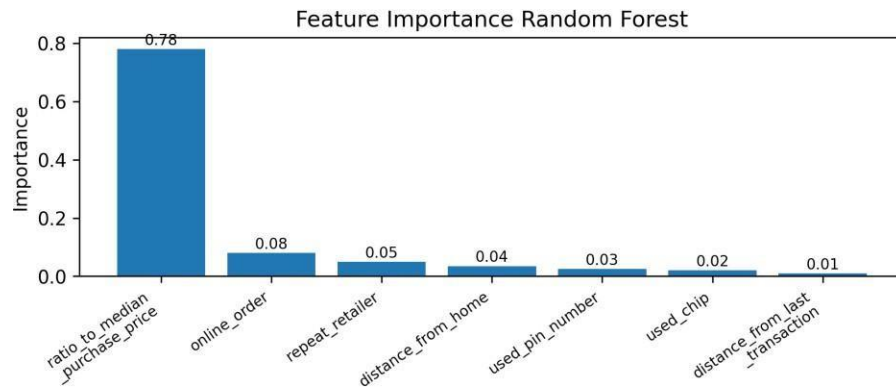
Nilai *AUC* sebesar 0,87 menunjukkan bahwa model memiliki kemampuan diskriminasi yang baik. Dalam konteks klasifikasi biner, *AUC* menggambarkan peluang model memberi skor lebih tinggi kepada sampel positif dibandingkan sampel negatif. Nilai 0,87 berarti model memiliki kualitas pemisahan kelas yang kuat, walaupun belum sempurna. Hasil ini mendukung penggunaan *Random Forest* sebagai model awal untuk *fraud detection*.



Gambar 5. ROC Curve model Random Forest dengan AUC 0,87

### G. Analisis Feature Importance

Analisis *feature importance* menunjukkan bahwa *ratio\_to\_median\_purchase\_price* menjadi fitur yang paling dominan. Fitur ini menggambarkan seberapa jauh nilai transaksi berbeda dari median pembelian. Perbedaan yang besar dapat menjadi sinyal adanya pola transaksi tidak wajar. Fitur *online\_order* dan *repeat\_retailer* juga memberi kontribusi karena transaksi digital dan pola retailer dapat membantu model mengenali perilaku pengguna.



Gambar 6. Feature importance pada model Random Forest

Tabel 8. Ringkasan Fitur Penting Model

| Peringkat | Fitur                                 | Kontribusi Umum                                                      |
|-----------|---------------------------------------|----------------------------------------------------------------------|
| 1         | <i>ratio_to_median_purchase_price</i> | Fitur paling dominan karena menunjukkan anomali nilai transaksi.     |
| 2         | <i>online_order</i>                   | Membantu mengenali pola transaksi berbasis <i>online</i> .           |
| 3         | <i>repeat_retailer</i>                | Memberi informasi apakah transaksi dilakukan pada retailer berulang. |
| 4         | <i>distance_from_home</i>             | Menunjukkan jarak transaksi dari lokasi rumah pengguna.              |
| 5         | <i>used_pin_number</i>                | Memberi sinyal keamanan autentikasi transaksi.                       |
| 6         | <i>used_chip</i>                      | Menunjukkan penggunaan chip kartu.                                   |
| 7         | <i>distance_from_last_transaction</i> | Memberi informasi perubahan lokasi dari transaksi sebelumnya.        |

### H. Pembahasan

Hasil penelitian menunjukkan bahwa *Random Forest* mampu menghasilkan performa tinggi pada data transaksi *online*. Akurasi sebesar 98% menunjukkan bahwa sebagian besar data uji diklasifikasikan dengan benar. Akan tetapi, akurasi tidak boleh menjadi satu-satunya dasar penilaian karena data yang

digunakan tidak seimbang. Pada *dataset* seperti ini, model dapat terlihat sangat baik karena berhasil mengenali kelas mayoritas, tetapi tetap gagal mengenali sebagian kelas *fraud*.

Perbedaan *precision* dan *recall* pada kelas *fraud* perlu dibaca secara hati-hati. *Precision* 100% berarti setiap transaksi yang diprediksi curang benar-benar curang. Namun, *recall* 72% berarti belum semua transaksi curang berhasil ditemukan. Dalam sistem deteksi kecurangan, *recall* kelas *fraud* sangat penting karena *false negative* dapat membuat transaksi curang tidak tertangani. Oleh karena itu, model ini kuat dari sisi ketepatan prediksi *fraud*, tetapi masih perlu ditingkatkan dari sisi sensitivitas.

Dominasi fitur *ratio\_to\_median\_purchase\_price* menunjukkan bahwa anomali nilai transaksi menjadi sinyal utama dalam klasifikasi. Temuan ini logis karena transaksi yang nilainya jauh dari pola median pembelian dapat menunjukkan perilaku tidak biasa. Sementara itu, fitur *online\_order* dan *repeat\_retailer* membantu model membaca konteks transaksi digital dan pola toko yang digunakan pengguna.

Dari sisi implementasi, *Random Forest* memiliki keunggulan karena mampu bekerja pada data besar dan menghasilkan *feature importance*. Informasi ini dapat membantu pengembang sistem dan analis keamanan memahami alasan prediksi model. Namun, model ini tetap memerlukan validasi lanjutan sebelum digunakan dalam sistem *real-time*. Evaluasi waktu eksekusi, integrasi sistem, keamanan data, dan pengujian pada data baru perlu dilakukan agar model layak diterapkan pada lingkungan produksi.

Keterbatasan penelitian ini terletak pada penggunaan data sekunder dan belum adanya pengujian langsung dalam sistem transaksi nyata. Selain itu, meskipun model menggunakan *class\_weight = balanced*, *recall* kelas *fraud* masih belum optimal. Penelitian lanjutan dapat menambahkan *SMOTE*, *undersampling*, threshold tuning, cost-sensitive learning, atau membandingkan *Random Forest* dengan *XGBoost*, *Gradient Boosting*, *Logistic Regression*, dan *Support Vector Machine*.

Tabel 9. Arah Pengembangan Model Deteksi Fraud

| Arah Pengembangan                            | Tujuan                                                                                                              |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Peningkatan <i>recall</i> kelas <i>fraud</i> | Mengurangi <i>false negative</i> agar transaksi curang tidak lolos deteksi.                                         |
| Threshold tuning                             | Menyesuaikan ambang prediksi agar model lebih sensitif terhadap kelas <i>fraud</i> .                                |
| Resampling data                              | Menggunakan <i>SMOTE</i> atau <i>undersampling</i> untuk mengurangi dampak <i>imbalanced data</i> .                 |
| Perbandingan algoritma                       | Menguji <i>XGBoost</i> , <i>Gradient Boosting</i> , <i>SVM</i> , dan <i>Logistic Regression</i> sebagai pembanding. |
| Uji <i>real-time</i>                         | Menilai waktu eksekusi dan kesiapan model pada sistem transaksi langsung.                                           |
| Explainable AI                               | Menambahkan <i>SHAP</i> atau metode penjelasan lain untuk memperkuat interpretasi.                                  |

## I. Pseudocode Implementasi Model

Agar alur komputasi lebih mudah dipahami, proses *Random Forest* dapat ditulis dalam bentuk pseudocode. Pseudocode ini tidak menggantikan kode program, tetapi menjelaskan urutan logis yang digunakan pada penelitian, mulai dari pembacaan data hingga evaluasi model.

Tabel 10. Pseudocode Implementasi Random Forest

| Langkah | Pseudocode                                                                                                                                  |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------|
| 1       | Import library: <i>Pandas</i> , <i>NumPy</i> , <i>Matplotlib</i> , <i>Scikit-learn</i> .                                                    |
| 2       | Load <i>dataset</i> <i>card_transdata.csv</i> .                                                                                             |
| 3       | Pisahkan <i>X</i> sebagai fitur dan <i>y</i> sebagai label <i>fraud</i> .                                                                   |
| 4       | Lakukan data cleaning, pemeriksaan outlier, dan validasi tipe data.                                                                         |
| 5       | Bagi <i>dataset</i> menjadi <i>X_train</i> , <i>X_test</i> , <i>y_train</i> , dan <i>y_test</i> dengan proporsi 80:20.                      |
| 6       | Inisialisasi <i>RandomForestClassifier</i> dengan <i>class_weight = balanced</i> .                                                          |
| 7       | Latih model menggunakan <i>X_train</i> dan <i>y_train</i> .                                                                                 |
| 8       | Prediksi data uji menggunakan <i>X_test</i> .                                                                                               |
| 9       | Hitung <i>accuracy</i> , <i>precision</i> , <i>recall</i> , <i>F1-score</i> , <i>confusion matrix</i> , <i>ROC Curve</i> , dan <i>AUC</i> . |
| 10      | Analisis <i>feature importance</i> untuk mengetahui fitur paling berpengaruh.                                                               |

## J. Interpretasi Rumus dalam Konteks Fraud Detection

Rumus voting mayoritas pada *Random Forest* menunjukkan bahwa keputusan akhir tidak ditentukan oleh satu pohon keputusan. Setiap tree memberi prediksi masing-masing, lalu kelas dengan suara terbanyak menjadi hasil akhir. Mekanisme ini penting karena data transaksi memiliki pola yang kompleks, sehingga satu model tunggal dapat terlalu sensitif terhadap *noise* atau pola lokal yang tidak mewakili keseluruhan data.

Rumus Gini Index digunakan untuk memilih pemisahan terbaik pada setiap node. Nilai Gini yang lebih kecil menunjukkan bahwa data pada node semakin homogen. Dalam konteks *fraud detection*, pemisahan yang baik berarti model mampu membedakan transaksi curang dan tidak curang berdasarkan fitur tertentu, misalnya rasio harga transaksi atau status *online\_order*.

Rumus *accuracy* menjelaskan proporsi seluruh prediksi yang benar. Namun, pada *dataset* tidak seimbang, *accuracy* harus dibaca bersama *recall* dan *confusion matrix*. Jika transaksi tidak curang jauh lebih banyak, model dapat memperoleh *accuracy* tinggi meskipun gagal menemukan sebagian transaksi *fraud*. Oleh karena itu, *recall* kelas *fraud* menjadi ukuran penting untuk menilai sensitivitas model.

Precision pada kelas *fraud* menunjukkan ketepatan model ketika memberi label curang. Nilai *precision* 100% pada penelitian ini menunjukkan bahwa semua transaksi yang diprediksi *fraud* memang termasuk *fraud*. Namun, *recall* 72% menunjukkan bahwa masih ada sebagian transaksi *fraud* yang tidak terdeteksi. Perbedaan ini menegaskan bahwa model perlu dioptimalkan bukan hanya untuk ketepatan, tetapi juga untuk kemampuan menemukan kasus *fraud* sebanyak mungkin.

*F1-score* digunakan untuk melihat keseimbangan antara *precision* dan *recall*. Pada kelas *fraud*, *F1-score* sebesar 84% menunjukkan performa yang cukup baik, tetapi belum maksimal. Jika sistem diarahkan untuk deteksi keamanan, peningkatan *recall* dapat lebih diprioritaskan meskipun konsekuensinya mungkin menambah *false positive*. Keputusan tersebut bergantung pada toleransi risiko bisnis dan biaya investigasi manual.

## K. Analisis Risiko Kesalahan Prediksi

Kesalahan prediksi pada sistem deteksi *fraud* memiliki dampak yang berbeda. False positive dapat membuat transaksi normal dianggap curang, sehingga pengguna mungkin mengalami penundaan transaksi atau perlu verifikasi tambahan. False negative lebih berbahaya karena transaksi curang tidak terdeteksi dan berpotensi menimbulkan kerugian finansial. Oleh karena itu, hasil *confusion matrix* perlu diterjemahkan menjadi risiko operasional, bukan hanya angka evaluasi.

Tabel 11. Makna Risiko pada Confusion Matrix

| Jenis Kesalahan | Makna dalam Sistem                          | Dampak                                                             | Prioritas Perbaikan                                          |
|-----------------|---------------------------------------------|--------------------------------------------------------------------|--------------------------------------------------------------|
| False positive  | Transaksi normal diprediksi <i>fraud</i> .  | Menambah beban review dan dapat mengganggu pengalaman pengguna.    | Perlu dikendalikan agar sistem tidak terlalu sensitif.       |
| False negative  | Transaksi <i>fraud</i> diprediksi normal.   | Transaksi curang lolos dari sistem dan dapat menimbulkan kerugian. | Harus menjadi prioritas utama dalam <i>fraud detection</i> . |
| True positive   | Transaksi <i>fraud</i> berhasil terdeteksi. | Membantu pencegahan kerugian dan memperkuat keamanan transaksi.    | Perlu dipertahankan dan ditingkatkan.                        |
| True negative   | Transaksi normal dikenali dengan benar.     | Menjaga kelancaran transaksi pengguna yang sah.                    | Perlu dipertahankan agar sistem tetap efisien.               |

## L. Implikasi Praktis Model

Secara praktis, model *Random Forest* dapat digunakan sebagai komponen awal dalam sistem pendukung keputusan. Sistem dapat memberi skor risiko pada setiap transaksi dan meneruskan transaksi berisiko tinggi ke proses verifikasi tambahan. Mekanisme ini dapat membantu lembaga keuangan, *e-commerce*, atau penyedia layanan pembayaran dalam mengurangi ketergantungan pada pemeriksaan manual.

Implementasi model tetap perlu memperhatikan batas penggunaan. Model tidak boleh dijadikan satu-satunya dasar pemblokiran transaksi tanpa prosedur validasi. Prediksi model sebaiknya digunakan sebagai sinyal awal yang perlu dikombinasikan dengan aturan bisnis, riwayat pengguna, autentikasi

tambahan, dan pemeriksaan analis. Pendekatan ini membuat sistem lebih aman dan lebih adil bagi pengguna.

Sebelum diterapkan dalam lingkungan *real-time*, model perlu diuji pada data baru dengan distribusi yang berbeda. Perubahan pola *fraud* dapat terjadi karena pelaku menyesuaikan strategi. Karena itu, model perlu dipantau secara berkala dan dilatih ulang ketika performanya menurun. Monitoring dapat dilakukan dengan melihat perubahan *accuracy*, *precision*, *recall*, *AUC*, jumlah *false negative*, dan proporsi transaksi yang masuk ke proses manual review.

Keamanan data juga harus menjadi perhatian utama. Dataset transaksi berpotensi mengandung informasi sensitif. Sistem prediksi perlu dilengkapi pengaturan hak akses, pencatatan aktivitas, enkripsi data, dan kebijakan penyimpanan hasil prediksi. Dengan demikian, pemanfaatan *machine learning* untuk *fraud detection* tidak hanya akurat secara teknis, tetapi juga aman dari sisi tata kelola data.

#### M. Rekomendasi Teknis Pengembangan Model

Pengembangan model perlu diarahkan pada peningkatan sensitivitas terhadap kelas *fraud*. Salah satu cara yang dapat dilakukan adalah threshold tuning. Pada model klasifikasi, keputusan kelas sering ditentukan berdasarkan ambang probabilitas 0,5. Ambang tersebut dapat diturunkan untuk membuat model lebih mudah memberi label *fraud*, sehingga *recall* kelas *fraud* dapat meningkat. Namun, strategi ini perlu dievaluasi karena dapat menambah *false positive*.

Teknik resampling juga dapat digunakan untuk memperbaiki distribusi data latih. *SMOTE* dapat menambah sampel sintesis pada kelas minoritas, sedangkan *undersampling* dapat mengurangi dominasi kelas mayoritas. Kedua pendekatan tersebut perlu diuji secara hati-hati agar model tidak kehilangan pola penting dari transaksi normal dan tidak membentuk pola sintesis yang kurang representatif.

Selain itu, pengembangan fitur perlu dilakukan dengan memperhatikan konteks perilaku pengguna. Fitur seperti frekuensi transaksi dalam periode tertentu, perubahan perangkat, jam transaksi, negara atau kota transaksi, pola merchant, dan riwayat kegagalan autentikasi dapat memberi sinyal tambahan. Penambahan fitur perilaku dapat membantu model mengenali pola *fraud* yang tidak cukup terlihat dari tujuh fitur awal.

Evaluasi model juga perlu dibuat lebih dekat dengan kebutuhan bisnis. Selain *accuracy* dan *AUC*, penelitian lanjutan dapat menghitung cost-sensitive evaluation. Biaya *false negative* biasanya lebih tinggi dibanding *false positive* karena transaksi curang yang lolos dapat menimbulkan kerugian langsung. Dengan pendekatan tersebut, pemilihan model tidak hanya didasarkan pada nilai statistik, tetapi juga dampak operasional.

Model yang akan digunakan pada sistem produksi perlu melalui validasi berlapis. Validasi pertama dilakukan pada data historis baru. Validasi kedua dilakukan melalui simulasi transaksi *real-time*. Validasi ketiga dilakukan dengan pemantauan berkala setelah sistem berjalan. Tahapan ini penting agar model tetap relevan ketika pola transaksi dan modus *fraud* berubah.

Tabel 12. Rekomendasi Teknis Pengembangan Model

| Strategi                | Tujuan                                                   | Catatan Implementasi                                                          |
|-------------------------|----------------------------------------------------------|-------------------------------------------------------------------------------|
| Threshold tuning        | Meningkatkan <i>recall</i> kelas <i>fraud</i> .          | Perlu memantau kenaikan <i>false positive</i> .                               |
| <i>SMOTE</i>            | Menambah representasi kelas minoritas.                   | Harus diuji agar tidak menambah pola sintesis yang bias.                      |
| Undersampling           | Mengurangi dominasi kelas mayoritas.                     | Berisiko membuang informasi penting dari transaksi normal.                    |
| Cost-sensitive learning | Memberi penalti lebih besar pada <i>false negative</i> . | Cocok untuk <i>fraud detection</i> karena kerugian <i>fraud</i> dapat tinggi. |
| Feature engineering     | Menambah fitur perilaku transaksi.                       | Memerlukan data tambahan dan kontrol privasi.                                 |
| Model monitoring        | Memantau penurunan performa setelah implementasi.        | Diperlukan karena pola <i>fraud</i> dapat berubah.                            |

#### 4. KESIMPULAN

Berdasarkan hasil penelitian, algoritma *Random Forest Classification* dapat diterapkan untuk mendeteksi kecurangan transaksi *online* menggunakan tujuh fitur transaksi dan satu label target. Model memperoleh *accuracy* sebesar 98% dan *AUC* sebesar 0,87, sehingga menunjukkan kemampuan klasifikasi yang kuat. Pada kelas tidak curang, model menghasilkan *precision* 97%, *recall* 100%, dan *F1-score* 99%. Pada kelas curang, model menghasilkan *precision* 100%, *recall* 72%, dan *F1-score* 84%. Hasil *confusion matrix* menunjukkan 182.519 *true negative*, 12.611 *true positive*, 0 *false positive*, dan 4.870 *false negative* dari 200.000 data uji. Temuan ini menunjukkan bahwa model sangat tepat ketika menandai transaksi sebagai *fraud*, tetapi masih perlu meningkatkan *recall* agar lebih banyak transaksi curang dapat terdeteksi. Fitur *ratio\_to\_median\_purchase\_price* menjadi variabel paling dominan dalam prediksi, diikuti *online\_order* dan *repeat\_retailer*. Dengan demikian, *Random Forest* berpotensi digunakan sebagai alat bantu deteksi kecurangan transaksi digital, tetapi pengembangan lanjutan tetap diperlukan melalui resampling, threshold tuning, validasi pada data baru, dan pengujian *real-time*.

### UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Program Studi Informatika, Fakultas Teknik dan Ilmu Komputer, Universitas Potensi Utama, serta seluruh pihak yang telah mendukung penyusunan penelitian dan konversi naskah skripsi menjadi artikel jurnal ini.

### REFERENSI

- [1] Almazroi, A. A., & Ayub, N. (2023). Online payment fraud detection model using machine learning techniques. *IEEE Access*, 11, 137188-137203.
- [2] Aburbeian, A. M., & Ashqar, H. I. (2023). Credit card fraud detection using enhanced random forest classifier for imbalanced data. In *International Conference on Advances in Computing Research* (pp. 605-616). Springer Nature Switzerland.
- [3] Benos, L., Tagarakis, A. C., Dolias, G., Berruto, R., Kateris, D., & Bochtis, D. (2021). Machine learning in agriculture: A comprehensive updated review. *Sensors*, 21(11), 3758.
- [4] Du, Q., & Zhai, J. (2024). Application of artificial intelligence sensors based on random forest algorithm in financial recognition models. *Measurement: Sensors*, 33, 101245.
- [5] Hu, T. (2025). Financial fraud detection system based on improved random forest and gradient boosting machine (GBM). *arXiv preprint arXiv:2502.15822*.
- [6] Ilham, M., Winarno, A., Lutfi, M., & Indrasetyaningsih, A. (2025). Handling imbalanced fraudulent transaction data using SMOTE-Tomek and Random Forest: A classification approach. *BEST: Journal of Applied Electrical, Science, & Technology*, 7(1).
- [7] Ibrahim, M. M., & Alfauzan, S. (2025). Analisis kinerja model machine learning untuk mendeteksi transaksi fraud pada sistem pembayaran online. *Jurnal Ilmiah Nusantara*, 2(3), 35-49.
- [8] Khakim, L., & Fadlilah, N. N. (2024). Analisis strategi Kepolisian Daerah Istimewa Yogyakarta dalam mengatasi kejahatan penipuan online di era Society 5.0. *Supremasi Hukum: Jurnal Penelitian Hukum*, 33(2), 124-136.
- [9] Lee, C. W., Fu, M. W., Wang, C. C., & Azis, M. I. (2025). Evaluating machine learning algorithms for financial fraud detection: Insights from Indonesia. *Mathematics*, 13(4), 600.
- [10] Rafid, A. M. (2023). Implementation of random forest algorithm for online transaction fraud detection. *Idea: Future Research*, 1(3), 106-112.
- [11] Silalahi, P. R., Daulay, A. S., Siregar, T. S., & Ridwan, A. (2022). Analisis keamanan transaksi e-commerce dalam mencegah penipuan online. *Profit: Jurnal Manajemen, Bisnis dan Akuntansi*, 1(4), 224-235.

- [12] Sopiyan, M., Fauziah, F., & Wijaya, Y. F. (2022). Fraud detection using random forest classifier, logistic regression, and gradient boosting classifier algorithms on credit cards. *JUITA: Jurnal Informatika*, 10(1), 77-87.
- [13] Pratama, S. F., & Wahid, A. M. A. (2025). Fraudulent transaction detection in *online* systems using *Random Forest* and *Gradient Boosting*. *Journal of Cyber Law*, 1(1), 88-115.
- [14] Raschka, S., Liu, Y. H., & Mirjalili, V. (2022). *Machine Learning* with PyTorch and Scikit-Learn: Develop *machine learning* and deep learning models with *Python*. Packt Publishing Ltd.
- [15] Vashistha, A., Tiwari, A. K., & Yadav, P. K. (2024). Enhancing banking security with leveraging *Random Forest* and *Gaussian Naive Bayes* for account *fraud detection*. In *International Conference on Information Technology* (pp. 209-219). Springer Nature Singapore.
- [16] Zhai, J. (2025). Automatic identification method for *fraudulent* users on *e-commerce* websites based on *Random Forest* algorithm. *Journal of Computational Methods in Sciences and Engineering*, 25(2), 1147-1154.
- [17] Federal Trade Commission. (2022). New analysis finds consumers reported losing more than \$1 billion in cryptocurrency scams since 2021. FTC News Events.
- [18] Pratiwi, N. I., & Prabowo, A. (2025). Analisis servicescape, hedonic lifestyle dan promotion intention terhadap keputusan pembelian konsumen pada Suara Coffee & Space. *RIGGS: Journal of Artificial Intelligence and Digital Business*, 4(3), 4547–4555. <https://doi.org/10.31004/riggs.v4i3.2656>
- [19] Riska, A., & Prabowo, A. (2025). Analisis social media marketing, servicescape, dan harga terhadap keputusan pembelian konsumen di Romansa Kopi. *RIGGS: Journal of Artificial Intelligence and Digital Business*, 4(3), 4917–4925. <https://doi.org/10.31004/riggs.v4i3.2710>
- [20] Arini, D. P., & Prabowo, A. (2025). Analisis customer experience dan customer trust terhadap keputusan pasien berkunjung kembali pada Klinik Alternatif Akupuntur Serumpun Bambu. *ANALISIS*, 15(2), 310–328. <https://doi.org/10.37478/als.v15i02.6497>
- [21] Prabowo, A., Adam, A. A., Subhan, Z. N., Tanjung, Y., Parhusip, A. A., Deviana, A., & Irwansyah. (2025). Sustainable business practices in coffee shops: The role of marketing innovation, digital marketing, and branding innovation through market development. *International Journal of Accounting and Economics Studies*, 12(6), 43–50. <https://doi.org/10.14419/p0k0pc78>
- [22] Akila, F., & Prabowo, A. (2025). Pengaruh customer experience, perceived product quality dan brand trust terhadap keputusan pembelian konsumen Dunkin Donuts Gatot Subroto. *ProBisnis: Jurnal Manajemen*, 16(5), 1157–1165. <https://ejournal.joninstitute.org/index.php/ProBisnis/article/view/1158>
- [23] Kurniawan, D., & Prabowo, A. (2025). Analisis customer relationship marketing, marketing communications dan service quality personal trainer terhadap tingkat kepuasan member pada Vizta Gym Cemara Asri Medan. *VALUE: Jurnal Ilmiah Akuntansi, Keuangan dan Bisnis*, 6(2), 392–407. <https://doi.org/10.36490/value.v6i2.2160>
- [24] Prabowo, A., Tanjung, Y., Enzelia, E. L., Bangun, R., Simarmata, H. M. P., & Wahyuni, E. S. (2025). Eksplorasi promosi berbasis social media marketing dan brand image: Identifikasi impulsive buying behaviour melalui customer engagement pada konsumen brand fashion ZARA di Kota Medan. *Jurnal Dunia Pendidikan*, 6(3), 727–747. <https://doi.org/10.55081/jurdip.v6i3.4431>
- [25] Prabowo, A., & Tarigan, T. D. (2025). Analisis servicescape, social media marketing dan customer experience terhadap minat berkunjung kembali konsumen Fore Coffee Citraland Helvetia Medan. *Jurnal Dunia Pendidikan*, 6(3), 996–1010. <https://doi.org/10.55081/jurdip.v6i3.4581>
- [26] Prabowo, A., Siburian, P., & Bangun, R. (2025). Repurchase intention among millennial coffee shop customers: Exploring key determinants. *International Journal of Accounting and Economics Studies*, 12(8), 761–769. <https://doi.org/10.14419/j7ch0q39>
- [27] Tanjung, S., & Prabowo, A. (2025). Analisis social media marketing dan customer relationship marketing terhadap kepuasan konsumen Sikologi Coffee. *Economic and Education Journal (Ecoducation)*, 7(3), 975–989. <https://doi.org/10.33503/ecoducation.v7i3.2345>
- [28] Rizki, S., Prabowo, A., & Pasaribu, E. S. (2025). Optimalisasi kinerja karyawan pada kawasan industri di

- Sumatera Utara: Peran work engagement dan employee experience melalui safety knowledge. *Economic and Education Journal (Ecoducation)*, 7(3), 1022–1038. <https://doi.org/10.33503/ecoducation.v7i3.2386>
- [29] Tarigan, R. R. M. T., Wahyuni, E. S., Prabowo, A., & Mauliza, P. (2026). Pengaruh pemasaran digital terhadap keputusan pembelian dengan citra merek sebagai variabel mediasi. *MARAS: Jurnal Penelitian Multidisiplin*, 4(1), 110–119. <https://doi.org/10.60126/maras.v4i1.1503>
- [30] Mahlia, M., & Prabowo, A. (2026). Analisis experiential marketing, word of mouth, dan online customer review terhadap keputusan pembelian pada PT. Alfa Scorpii. *RIGGS: Journal of Artificial Intelligence and Digital Business*, 5(1), 14596–14606. <https://doi.org/10.31004/riggs.v5i1.8083>
- [31] Dalimunthe, S. M., & Pohan, Y. A. (2025). Pengaruh budaya digital, pengembangan sumber daya manusia (SDM) dan lingkungan kerja fisik terhadap kinerja pegawai Dinas Ketenagakerjaan Kota Medan. *RIGGS: Journal of Artificial Intelligence and Digital Business*, 4(3), 7004–7014. <https://doi.org/10.31004/riggs.v4i3.3050>
- [32] Tambunan, A. M., & Pohan, Y. A. (2025). Pengaruh inovasi produk, free layanan after sales dan kualitas informasi produk di website terhadap keputusan pembelian mesin Inkjet PT. Megasatria Hiticher. *RIGGS: Journal of Artificial Intelligence and Digital Business*, 4(3), 7412–7422. <https://doi.org/10.31004/riggs.v4i3.3107>
- [33] Delvin, S., & Pohan, Y. A. (2025). Pengaruh komitmen afektif, komitmen berkelanjutan dan komitmen normatif terhadap kinerja karyawan PT Navya Retail Indonesia. *RIGGS: Journal of Artificial Intelligence and Digital Business*, 4(3), 7540–7550. <https://doi.org/10.31004/riggs.v4i3.3134>
- [34] Zai, S., & Pohan, Y. A. (2025). Pengaruh sanksi keterlambatan, biaya administrasi dan tarif jasa simpan terhadap kepuasan nasabah dalam menggunakan jasa gadai pada PT. Sentral Gadai Persada. *RIGGS: Journal of Artificial Intelligence and Digital Business*, 4(3). <https://doi.org/10.31004/riggs.v4i3.3284>
- [35] Devini, S. Z., & Pohan, Y. A. (2025). Pengaruh kualitas pelayanan, kualitas produk dan fasilitas terhadap kepuasan pelanggan Lazatto Chicken & Burger cabang UMSU. *Jurnal Daya Saing*, 11(3), 899–905. <https://doi.org/10.35446/dayasaing.v11i3.2504>
- [36] Zulnawati, S. E., & Pohan, Y. A. (2026). Pengaruh perceived ease of use, brand trust dan customer experience terhadap minat pengguna Maxim di Kota Medan. *Jurnal Akutansi Manajemen Ekonomi Kewirausahaan (JAMEK)*, 6(1), 112–120. <https://doi.org/10.47065/jamek.v6i1.2285>
- [37] Rezzaini, H., Kadariah, S., & Riski, B. (2025). Pengaruh pembiayaan murabahah dan literasi keuangan terhadap kesejahteraan nasabah UMKM. *Jurnal Riset Perbankan Syariah*, 4(2), 143–152. <https://doi.org/10.29313/jrps.v4i2.8726>
- [38] Nazli, P., Kadariah, S., & Sari, S. P. (2026). Model peningkatan minat menabung generasi Z di bank syariah melalui media sosial dan edukasi digital untuk penguatan ekosistem keuangan. *Journal of Science and Social Research*, 9(3), 4999–5005. <https://doi.org/10.54314/jsr.v9i3.6723>
- [39] Sipahutar, E., Asshidiq, H., Kadariah, S., Murtani, A., Nazli, P., & Trihapsari, M. (2026). Integrasi pengetahuan, religiusitas, promosi dan minat dalam keputusan menabung berbasis perilaku individu: Pendekatan multidisiplin (MSDM, psikologi, perbankan syariah, dan akuntansi). *Jurnal Ilmiah Edunomika*, 10(2). <https://doi.org/10.29040/jie.v10i2.19873>
- [40] Reza, F., & Nazli, P. (2025). SWOT analysis in the marketing strategy of IB Mudarabah Deposit products at PT. Bank Sumut KCP Syariah Karya Medan. *Digital Business: Tren Bisnis Masa Depan*, 16(4), 171–178. <https://ejournal.cria.or.id/index.php/db/article/view/357>
- [41] Andira, M. F., & Ridwan, M. (2025). The influence of service quality, transparency, and religiosity on PT Bank Mandiri employees' interest in donation to Ziswaf at The Mandiri Amal Insani Zakat (LAZ) Institution Medan Representative. *BISEI: Jurnal Bisnis dan Ekonomi Islam*, 10(2), 117–130. <https://doi.org/10.33752/bisei.v10i2.10758>
- [42] Ainayah, D., Hutagalung, M. K., Riski, B., & Arafah, S. (2025). Pengaruh perceived value dan perceived quality terhadap loyalitas nasabah pembiayaan KPR IB Griya pada PT Bank Sumut Syariah KCPSY Hamparan Perak. *RIGGS: Journal of Artificial Intelligence and Digital Business*, 4(4), 2015–2021. <https://doi.org/10.31004/riggs.v4i4.3561>
- [43] Daulay, Z., Riski, B., & Hutagalung, M. K. (2025). Analisis implementasi metode pemasaran direct selling

- pada produk talangan umroh di PT. Bank Sumut Syariah Kantor Cabang Pembantu Hamparan Perak. RIGGS: Journal of Artificial Intelligence and Digital Business, 4(4), 2133–2143. <https://doi.org/10.31004/riggs.v4i4.3551>
- [44] Rahman, R. J., Miko, J., & Rizki, B. (2025). The impact of mobile banking services on customer satisfaction in the digital era at PT. Bank Sumut Syariah KCP Hamparan Perak. RIGGS: Journal of Artificial Intelligence and Digital Business, 4(4), 5940–5946. <https://doi.org/10.31004/riggs.v4i4.4135>
- [45] Rezzaini, H., Kadariah, S., & Riski, B. (2025). Pengaruh pembiayaan murabahah dan literasi keuangan terhadap kesejahteraan nasabah UMKM. Jurnal Riset Perbankan Syariah, 4(2), 143–152. <https://doi.org/10.29313/jrps.v4i2.8726>
- [46] Daulay, Z., Riski, B., & Hutagalung, M. K. (2025). Analisis implementasi metode pemasaran direct selling pada produk talangan umroh di PT. Bank Sumut Syariah Kantor Cabang Pembantu Hamparan Perak. RIGGS: Journal of Artificial Intelligence and Digital Business, 4(4), 2133–2143. <https://doi.org/10.31004/riggs.v4i4.3551>
- [47] Alfinsyah, R., & Murtani, A. (2025). Analysis of the use of QRIS as financial technology among millennials: A case study at Warkop Kita 2 and Warkop Agam. Digital Business: Tren Bisnis Masa Depan, 16(4), 164–170. <https://doi.org/10.59651/digital.v16i4.355>
- [48] Eka Putra, S., Nurmala Sari, T., Simatupang, J., Murtani, A., & Tanjung, Y. (2025). Analysis of the benefits of the 7P marketing mix strategy on the brand image of Butong Tea at PT Perkebunan Nusantara IV Bah Butong. Jurnal Ilmiah Sosio-Ekonomika Bisnis, 28(2), 30–37. <https://doi.org/10.22437/jiseb.v28i02.41506>