Indonesian Journal on Data Science
ISSN 2987-7423 - Vol. 3, No. 2, November 2025, hlm 97-107

Deteksi Dini Fraud pada Layanan Keuangan Digital Menggunakan Metode Random Forest

Amanda Sifaul Zanah[a,1]*, Belva Calista [b,2], Wiwiek Nurkomala Dewi[c,3], Petrus Sokibi[d,4]

[a,b,c,d] Catur Insan Cendekia University, Jl Kesambi 203, kota Cirebon, 45133, Indonesia
[1]amanda.zanah.ti.23@cic.ac.id*; [2]belva.calista.ti.23@cic.ac.id; [3]wiwiek.nurkomala.dewi@cic.ac.id; [4]petrus.sokibi@cic.ac.id

* corresponding author

ABSTRACT

Layanan keuangan digital yang terus berkembang telah memberikan kemudahan dalam melakukan transaksi finansial. Namun, kemajuan ini juga disertai meningkatnya risiko penipuan *(fraud)*, yang dapat merugikan baik individu maupun institusi. Oleh karena itu, diperlukan langkah pencegahan yang efektif, salah satunya melalui penerapan teknik *data mining*. Penelitian ini memanfaatkan *data mining* sebagai alat untuk deteksi dini transaksi mencurigakan pada layanan keuangan digital. Metode yang digunakan adalah klasifikasi seperti *Random Forest*, *Decision Tree*, dan *Neural Network*, dengan studi kasus berdasarkan dataset transaksi finansial dari sebuah platform digital. Proses analisis melibatkan penerapan algoritma *machine learning* untuk membangun model prediksi yang mampu membedakan transaksi normal dan mencurigakan. Hasil penelitian menunjukkan bahwa model *Random Forest* yang dikembangkan memiliki tingkat akurasi tinggi yaitu 100% dan *F1-Score* 87,1% dalam mendeteksi *fraud* secara tepat tanpa menghasilkan kesalahan prediksi, sehingga dapat digunakan sebagai sistem peringatan dini untuk mencegah kerugian lebih lanjut. Kesimpulan ini menunjukkan bahwa *data mining* berpotensi besar dalam meningkatkan keamanan layanan keuangan digital melalui deteksi dan mitigasi *fraud* secara proaktif.

ARTICLE INFO

Article history
Received: 25 Januari 2025
Revised: 28 April 2025
Accepted: 26 November 2025

Keywords
Data-Mining
Deteksi-Fraud
Layanan Keuangan-Digital
Machine-Learning

I. Pendahuluan

Transformasi digital di sektor keuangan telah berkembang pesat dalam beberapa tahun terakhir. Perkembangan teknologi dan meningkatnya adopsi perangkat digital mendorong terciptanya layanan keuangan digital yang semakin mudah diakses. Layanan ini mencakup berbagai aktivitas seperti *mobile banking*, *e-wallet*, *transaksi online*, pembayaran elektronik, pinjaman *peer-to-peer*, hingga layanan investasi digital. Kemudahan ini memberikan manfaat signifikan bagi konsumen dan industri, seperti efisiensi proses transaksi, kemudahan akses, serta pengurangan biaya operasional.

Namun, seiring dengan pesatnya adopsi teknologi, ancaman terhadap keamanan transaksi keuangan digital juga meningkat. Kasus penipuan atau *fraud* menjadi salah satu tantangan terbesar yang dihadapi oleh penyedia layanan keuangan digital. *Fraud* dapat berwujud dalam berbagai bentuk, seperti pencurian identitas, penggunaan kartu kredit curian, transaksi tidak sah, hingga penyalahgunaan akun [1]. Menurut OJK, pengaduan terkait penipuan layanan keuangan digital terus meningkat dari tahun ke tahun [2]. Melalui Laporan Indonesia Anti-Scam Centre sejak awal beroperasi hingga 23 Maret 2025 tercatat 74.243 laporan dengan nilai kerugian mencapai 1,4 triliun

rupiah [3]. Data ini menunjukkan bahwa fraud pada sistem keuangan digital telah menjadi isu nasional. Kehadiran ancaman *fraud* ini menimbulkan kerugian finansial yang besar, tidak hanya bagi individu pengguna, tetapi juga bagi institusi keuangan itu sendiri [4].

Pentingnya deteksi dini terhadap aktivitas *fraud* menjadi faktor kunci dalam menjaga kepercayaan konsumen dan memastikan keamanan transaksi. Metode deteksi konvensional yang berbasis pada aturan dan analisis manual sering kali tidak cukup efektif dalam menghadapi *volume* data transaksi yang besar dan kompleks [5]. Oleh karena itu, diperlukan pendekatan yang lebih canggih dan otomatis dalam mendeteksi *fraud* [6].

Tantangan utama dalam mendeteksi *fraud* adalah mengenali pola-pola transaksi yang mencurigakan di antara ribuan bahkan jutaan transaksi yang dilakukan setiap hari. *Fraud* sering kali disamarkan sebagai transaksi normal, sehingga deteksi yang cepat dan akurat menjadi tugas yang sangat sulit. Metode manual tidak hanya memakan waktu, tetapi juga rentan terhadap kesalahan. Selain itu, *fraudster* (pelaku penipuan) terus mengembangkan teknik baru yang membuat deteksi menjadi semakin rumit.

Data mining merupakan solusi yang tepat untuk mengatasi tantangan ini. Dengan kemampuan untuk menganalisis data dalam jumlah besar dan menemukan pola yang tidak mudah dikenali secara manual, *data mining* memberikan pendekatan yang lebih efektif dan efisien [4]. Teknik-teknik seperti klasifikasi, *clustering*, dan deteksi anomali dapat digunakan untuk mendeteksi pola transaksi yang mencurigakan dan mengidentifikasi potensi *fraud* [7].

Beberapa penelitian terdahulu telah membahas penerapan data mining dalam mendeteksi aktivitas *fraud* pada transaksi digital. Penelitian oleh [8] menunjukkan bahwa akurasi pendeteksi penipuan dapat meningkat hingga 90% dengan tingkat *false positive* rendah menggunakan *Random Forest*. Sehingga algoritma ini sangat cocok untuk deteksi penipuan karena mampu mengelola data tidak seimbang. Selain itu, penelitian [9] menunjukkan *Random Forest* memberikan performa terbaik pada akurasi dan *recall* serta dapat diandalkan melalui pendekatan *ensemble learning* untuk meningkatkan deteksi penipuan pada transaksi digital.

Penelitian ini berfokus pada deteksi *fraud* menggunakan *data mining* berbasis *supervised learning*, di mana data transaksi yang sudah diberi label "*fraud*" atau "*non-fraud*" digunakan untuk melatih model. Teknik klasifikasi, seperti *Random Forest*, *Decision Tree*, dan *Neural Network*, digunakan untuk membangun model deteksi *fraud*. Studi kasus dilakukan menggunakan dataset transaksi yang mencakup atribut-atribut standar dalam layanan keuangan digital.

Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi nyata dalam meningkatkan keamanan layanan keuangan digital melalui pemanfaatan *data mining* untuk deteksi dini *fraud*. Adopsi teknologi ini akan memberikan perlindungan yang lebih baik bagi konsumen sekaligus membantu industri keuangan dalam mengelola risiko operasional yang muncul akibat ancaman penipuan.

2. Tinjauan Pustaka

2.1. *Data Mining*

Data mining adalah proses penemuan pola atau informasi yang berguna dari dataset yang besar [10]. Tujuan utama dari *data mining* adalah untuk mengekstraksi informasi yang bermanfaat dari data mentah dengan menggunakan berbagai teknik statistik, matematika, dan algoritma *machine learning* [11]. *Data mining* dalam konteks deteksi *fraud* berfokus pada identifikasi pola transaksi yang tidak biasa atau mencurigakan yang dapat menunjukkan aktivitas penipuan.

Beberapa teknik *data mining* yang umum digunakan dalam deteksi *fraud* [12], [13]meliputi:

1. **Klasifikasi (*Classification*)**: Teknik yang digunakan untuk memprediksi label dari data baru berdasarkan model yang dilatih. Model ini menggunakan data dengan label yang sudah diketahui untuk mengidentifikasi apakah suatu transaksi termasuk "*fraud*" atau "*non-fraud*".
2. ***Clustering***: Teknik yang mengelompokkan data tanpa menggunakan label yang sudah diketahui, sehingga dapat digunakan untuk mendeteksi pola yang tidak biasa (anomali).

3. **Deteksi Anomali (*Anomaly Detection*)**: Teknik yang digunakan untuk mengidentifikasi data yang berbeda secara signifikan dari pola umum, yang dapat menunjukkan aktivitas *fraud*.

2.2. Klasifikasi dengan *Machine Learning*

Metode klasifikasi adalah salah satu pendekatan yang paling umum digunakan untuk mendeteksi *fraud*. Model klasifikasi berfungsi untuk mengelompokkan data berdasarkan beberapa variabel input (*features*) dan memberikan *output* berupa kelas prediksi [14]. Algoritma yang sering digunakan untuk deteksi *fraud* meliputi: *Logistic Regression, Decision Tree, Random Forest, Support Vector Machine (SVM), Neural Network*

Berikut adalah beberapa rumus yang digunakan dalam evaluasi model klasifikasi [15]:

1. *Accuracy*: Mengukur proporsi prediksi yang benar dibandingkan dengan total data.

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

TP (*True Positive*) = Transaksi *fraud* yang terdeteksi dengan benar.

TN (*True Negative*) = Transaksi normal yang terdeteksi dengan benar.

FP (*False Positive*) = Transaksi normal yang salah terdeteksi sebagai *fraud*.

FN (*False Negative*) = Transaksi *fraud* yang tidak terdeteksi.

2. *Precision*: Mengukur proporsi prediksi *fraud* yang benar terhadap semua prediksi *fraud*.

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

3. *Recall*: Mengukur proporsi transaksi *fraud* yang terdeteksi dengan benar dibandingkan dengan total transaksi *fraud* sebenarnya.

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

4. *F-1 Score*: Merupakan rata-rata harmonis dari *Precision* dan *Recall*. *F-1 Score* memberikan gambaran gambaran keseimbangan antara *Precision* dan *Recall*.

$$Recall = 2\frac{Precision\,.Recall}{Precision + Recall} \quad (4)$$

2.3. *Random Forest*

Random Forest adalah algoritma *machine learning* berbasis *ensemble* yang terdiri dari beberapa pohon keputusan (*decision tree*). Setiap pohon keputusan dilatih menggunakan subset dari dataset, dan hasil akhir diperoleh melalui voting mayoritas dari pohon-pohon tersebut [16]. *Random Forest* cocok untuk deteksi *fraud* karena mampu menangani data yang kompleks dengan variabel *input* yang beragam [9].

Algoritma Dasar *Random Forest* [16]:

1. Bangun N pohon keputusan menggunakan subset acak dari dataset.
2. Setiap pohon menggunakan fitur acak yang berbeda untuk mengurangi
3. Lakukan voting untuk menentukan kelas akhir berdasarkan hasil prediksi dari setiap pohon.

Keuntungan *Random Forest* [16]:

- *Robust* terhadap *overfitting* karena menggunakan banyak pohon.
- Efisien untuk dataset yang besar dan fitur yang kompleks.
- Kemampuan interpretasi yang baik melalui analisis *feature importance*.

2.4. Evaluasi Model dengan *Confusion Matrix*

Confusion Matrix adalah alat yang digunakan untuk mengevaluasi kinerja model klasifikasi [17]. Matriks ini menunjukkan hasil prediksi dibandingkan dengan tabel asli. Berikut adalah bentuk umum dari *Confusion Matrix* yang ditunjukkan pada Tabel 1.

Table 1. Confusion Matrix

	Prediksi Fraud (1)	***Prediksi Non-Fraud (0)***
Fraud (1)	*True Positive*	*False Negative*
Non-Fraud (0)	*False*	*True Negative*

True Positive berarti model mendeteksi *fraud* dengan benar, sedangkan *False Positive* berarti model salah mendeteksi transaksi normal sebagai *fraud*. Interpretasi dari *Confusion Matrix* membantu dalam memahami seberapa baik model mendeteksi *fraud* tanpa perlu banyak memunculkan alarm palsu (*false positive*).

2.5. *Area Under the Curve* (AUC) dan *Receiver Operating Characteristic* (ROC)

ROC Curve adalah grafik yang menggambarkan kinerja model klasifikasi dengan memplot hubungan *True Positive Rate* (TPR) dan *False Positive Rate* (TPR) pada berbagai *threshold* [18]. Area di bawah kurva (AUC) mengukur seberapa baik model dapat membedakan antara kelas positif dan negative [19].

- *True Positive Rate* (TPR) (juga disebut *Recall*):

$$TPR = \frac{TP}{TP + FN} \tag{5}$$

- *False Positive Rate* (FPR):

$$FPR = \frac{FP}{FP + TN} \tag{6}$$

Semakin besar nilai AUC (mendekati 1), semakin baik performa model mendekari *fraud*.

2.6. Algoritma *Logistic Regression*

Logistic Regression adalah model statistik yang digunakan untuk memprediksi probabilitas suatu kejadian berdasarkan variabel *input* [18]. Model ini sering digunakan untuk klasifikasi *binary*, seperti deteksi *fraud* ("*fraud*" vs "*non-fraud*").

Rumus Prediksi dalam *Logistic Regression* [18]:

$$p(y = 1|X) = \frac{1}{1 + e^{-(\beta_0 + \beta_1 X_1 + \beta_2 X_2 + \ldots\ldots + \beta_n X_n)}} \tag{7}$$

Keterangan:

P(y = 1|X) adalah probabilitas prediksi bahwa transaksi adalah *fraud*.

X_i adalah fitur *input*

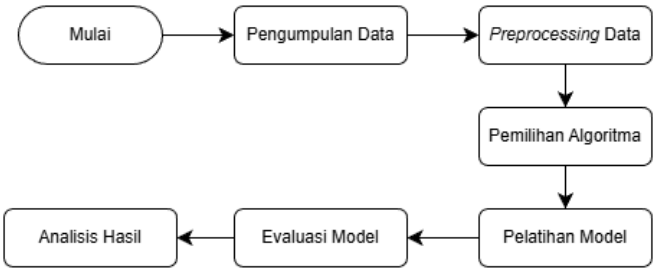
β_i adalah koefisien regresi yang diestimasi dari data

Dengan menggunakan *Logistic Regression*, kita dapat menentukan seberapa besar pengaruh masing-masing variabel (seperti jumlah transaksi, lokasi, waktu) terhadap kemungkinan terjadinya *fraud*. Bagian ini memberikan gambaran teoritis mengenai berbagai konsep dan metode yang digunakan dalam deteksi *fraud* dengan *data mining*.

3. Metodologi Penelitian

3.1. Desain Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan metode eksperimen untuk mengevaluasi performa model deteksi *fraud* yang dibangun menggunakan teknik *data mining*. Tahapan penelitian dapat dilihat pada Gambar 1.



Gambar 1. Tahapan Penelitian

Proses penelitian melibatkan langkah-langkah berikut:

1. **Pengumpulan Data**: Data transaksi keuangan dikumpulkan dari sumber yang relevan.
2. ***Preprocessing* Data**: Data yang dikumpulkan diproses untuk menghilangkan *noise* dan menyiapkannya untuk analisis.
3. **Pemilihan Algoritma**: Beberapa algoritma *machine learning* dipilih untuk mendeteksi *fraud*.
4. **Pelatihan Model (*Model Training*)**: Model dilatih menggunakan dataset yang sudah dibersihkan.
5. **Evaluasi Model**: Model dievaluasi menggunakan metrik performa yang sesuai.
6. **Analisis Hasil**: Hasil analisis disajikan dalam bentuk tabel, grafik, dan interpretasi.

3.2. Pengumpulan Data

Data yang digunakan dalam penelitian ini merupakan data transaksi keuangan yang mencakup informasi berikut:

- **ID Transaksi**: Nomor unik transaksi.
- **Tipe Transaksi**: Jenis transaksi yang digunakan *user*.
- **Nominal**: Jumlah uang yang ditransaksikan.
- **Frekuensi Transaksi/Jam**: Waktu transaksi dilakukan (dalam menit sejak awal hari).
- **Jarak Lokasi Transaksi**: Lokasi geografis dari satu transaksi ke transaksi lain.
- **Selisih Waktu**: Toko atau penyedia layanan dimana transaksi dilakukan.
- **Indikasi *Fraud***: Indikator apakah transaksi merupakan *fraud* (1) atau *non-fraud* (0).

Sumber data dapat berupa dataset publik yang sudah ada (misalnya dataset dari Kaggle atau repositori publik lainnya), data transaksi nyata dari institusi keuangan yang bersedia berbagi data untuk keperluan penelitian atau data *dummy* yang digunakan sebagai contoh kasus perhitungan *data mining* ini. Data ini kemudian diolah dan disiapkan untuk analisis lebih lanjut.

3.3. *Preprocessing Data*

Preprocessing data melibatkan beberapa tahap penting untuk memastikan kualitas data yang akan digunakan dalam analisis:

1. **Pembersihan Data (*Data Cleaning*)**:
    - ***Handling Missing Values***: Mengganti atau menghapus nilai yang hilang (*missing values*) dengan teknik seperti *mean imputation* atau *median imputation*.
    - **Menghapus Duplikasi**: Menghapus data transaksi yang duplikat.
    - ***Outlier Detection***: Mengidentifikasi dan menangani data yang keluar dari rentang normal menggunakan teknik seperti *z-score* atau IQR (*Interquartile Range*).

2. **Transformasi Data (*Data Transformation*)**:
    - ***Encoding* Data Kategorikal**: Mengubah data kategorikal seperti lokasi atau *merchant* menjadi bentuk numerik menggunakan teknik *One-Hot Encoding* atau *Label Encoding*.
    - **Normalisasi Data**: Normalisasi data numerik agar berada dalam skala yang sama menggunakan metode seperti *Min-Max Scaling* atau *Z-Score Scaling*.
3. **Pembagian Dataset (*Train-Test Split*)**:
    - Data transaksi dibagi menjadi dua bagian: 80% untuk *data training* dan 20% untuk *data testing*.
    - Pembagian dilakukan secara acak untuk memastikan bahwa *data training* dan *testing representatif* terhadap populasi data.

3.4. Pemilihan Algoritma

Algoritma yang dipilih untuk deteksi *fraud* dalam penelitian ini adalah:

1. ***Random Forest***: Metode *ensemble* berbasis pohon keputusan yang dapat menangani data dengan variabel kompleks.
2. ***Logistic Regression***: Model statistik untuk klasifikasi *binary*, yang sederhana dan interpretatif.

Setiap algoritma akan diuji kinerjanya untuk menentukan model terbaik dalam mendeteksi transaksi *fraud*.

3.5. Pelatihan Model (*Model Training*)

Model dilatih menggunakan *dataset training* yang sudah dipreproses. Proses pelatihan melibatkan beberapa langkah:

1. **Pemilihan *Hyperparameter***: Mencari kombinasi parameter terbaik untuk setiap algoritma (misalnya jumlah pohon pada *Random Forest* atau parameter regulasi CCC pada SVM) menggunakan teknik *Grid Search* atau *Random Search*.
2. ***Cross-Validation***: Menggunakan metode *K-Fold Cross Validation* (misalnya K=5 atau K=10) untuk memvalidasi model. Dalam metode ini, dataset *training* dibagi menjadi K bagian, di mana satu bagian digunakan untuk validasi dan sisanya untuk *training* secara bergantian.
3. **Pelatihan Ulang (*Fine-tuning*)**: Melakukan penyesuaian ulang model berdasarkan hasil *cross-validation* untuk meningkatkan akurasi dan mengurangi kesalahan prediksi.

3.6. Evaluasi Model

Model yang sudah dilatih akan dievaluasi menggunakan *dataset testing* yang terpisah. Evaluasi dilakukan dengan menggunakan beberapa metrik performa berikut:

1. ***Confusion Matrix***: Mengukur jumlah *True Positive* (TP), *True Negative* (TN), *False Positive* (FP), dan *False Negative* (FN).
2. **Metrik Evaluasi**:
    - ***Accuracy***: Proporsi prediksi yang benar.
    - ***Precision***: Ketepatan prediksi transaksi *fraud*.
    - ***Recall***: Kemampuan model untuk mendeteksi semua transaksi *fraud*.
    - ***F1-Score***: Kombinasi harmonis antara *Precision* dan *Recall*.
    - **ROC *Curve* (*Receiver Operating Characteristic*)**: Grafik yang menggambarkan kemampuan model dalam membedakan antara kelas *fraud* dan *non-fraud*.
    - **AUC (*Area Under Curve*)**: Luas di bawah kurva ROC yang menunjukkan kemampuan diskriminasi model.

3.7. Analisis Hasil

Hasil yang diperoleh dari evaluasi model akan dianalisis lebih lanjut:

1. **Identifikasi Faktor Kunci**: Melihat fitur mana yang paling berpengaruh dalam menentukan prediksi *fraud*. Pada *Random Forest*, dapat digunakan *Feature Importance* untuk mengidentifikasi variabel yang memiliki pengaruh terbesar terhadap keputusan model.

2. **Evaluasi Performa Algoritma**: Membandingkan hasil evaluasi dari berbagai algoritma yang diuji untuk menentukan algoritma terbaik. Ini dilakukan dengan melihat akurasi, *precision*, *recall*, *F1-score*, serta ROC dan AUC.
3. **Visualisasi Data**: Menyajikan hasil analisis dalam bentuk grafik dan visualisasi untuk memahami pola *fraud* yang terdeteksi.

3.8. Validasi dan Uji Signifikansi

Untuk memastikan bahwa hasil penelitian valid dan dapat digeneralisasi:

1. **Validasi Model**: Menggunakan dataset yang berbeda atau data uji eksternal untuk menguji performa model di luar dataset yang digunakan untuk pelatihan.
2. **Uji Signifikansi Statistik**: Menggunakan uji statistik seperti *Chi-Square Test* atau *T-Test* untuk menentukan apakah hasil dari algoritma lebih baik secara signifikan dibandingkan dengan metode deteksi konvensional.

4. Hasil dan Pembahasan

4.1. Deskripsi Kasus

Bank Calistung merupakan institusi keuangan yang menyediakan layanan transaksi digital. Selama beberapa bulan terakhir, terjadi peningkatan kasus penipuan (*fraud*) yang berdampak pada kerugian finansial perusahaan dan kepercayaan pelanggan. Oleh karena itu, Bank Calistung ingin mengembangkan model prediksi yang dapat mendeteksi transaksi mencurigakan secara *real-time* menggunakan *data mining*. Data yang digunakan dalam penelitian ini diperoleh dari dataset yang berjudul "Bank Transaction Fraud Detection" yang tersedia di Kaggle.

Dataset yang digunakan dalam studi kasus ini berjumlah 200.000 *row*. Dataset tersebut berisi data transaksi keuangan yang mencakup ID Transaksi, Tipe Transaksi, Nominal, Frekuensi Transaksi/Jam, Jarak Lokasi Transaksi, Selisih Waktu, Indikasi Fraud. Rasio data antara *fraud* dan *non-fraud* adalah 1:1 dalam dataset yang digunakan, memungkinkan evaluasi model pada skenario ideal. Berikut sampel dataset yang dapat dilihat pada Table 2.

Table 2. Contoh Data Transaksi

ID Transaksi	Tipe Transaksi	Nominal (Rp.)	Frekuensi Transaksi/Jam	Jarak Lokasi Transaksi (KM)	Selisih Waktu (Menit)
1	Payment	137.000	2	3	40
2	Payment	379.000	1	5	55
3	Transfer	1.020.000	3	210	2
4	Cash Out	650.000	4	103	4
5	Payment	499.000	5	6	70
6	Payment	75.000	3	2	60
7	Payment	90.000	1	1	43
8	Debit	515.000	6	130	3
9	Debit	729.000	2	155	3
10	Cash Out	2.000.000	1	230	4

4.2. Preprocessing Data

Data yang telah dikumpulkan dilakukan *preprocessing* data. Tahapan ini meliputi

1. ***Handling Missing Values***: Hasil pemeriksaan *missing values* menunjukkan bahwa dataset tidak memiliki nilai yang hilang. Oleh karena itu, setelah dilakukan *handling missing values*, tidak terjadi perubahan pada dataset. Hal ini menunjukkan bahwa data transaksi sudah lengkap dan konsisten.
2. ***Encoding Data* Kategorikal**: Kolom Indikasi *Fraud* diubah menjadi bentuk numerik menggunakan *One-Hot Encoding*.

3. ***Scaling***: Kolom Nominal Transaksi dan Jarak Transaksi dinormalisasi menggunakan *Min-Max Scaling*. Dimana nilainya berada pada rentang 0 hingga 1.
4. **Penyesuaian Data dan Ketidakseimbangan Kelas**: Mengingat rasio asli antara transaksi *fraud* dan *non-fraud* sangat tidak seimbang dimana 189.912 transaksi *non-fraud* dan 10.088 transaksi *fraud*. Setelah dilakukan *undersampling* pada kelas *non-fraud,* jumlah transaksi pada kedua kelas menjadi seimbang, masing-masing 10.088 transaksi, sehingga dataset kini memiliki rasio 1:1 antara *fraud* dan *non-fraud*.

4.3. Algoritma yang Digunakan

Algoritma yang digunakan dalam studi kasus ini adalah *Random Forest* dan *Logistic Regression*. *Random Forest* dipilih karena kemampuannya menangani data yang kompleks, sedangkan *Logistic Regression* dipilih karena interpretasi yang mudah terhadap pengaruh fitur terhadap prediksi.

4.4. *Training Model*

Model dilatih menggunakan dataset pelatihan dengan parameter yang telah ditentukan. Pembagian data dilakukan menggunakan *train test split* menjadi 80% data *training* dan 20% data *testing*. Evaluasi ditentukan pada dataset pengujian untuk memastikan generalisasi model pada data baru. Proses *training* dilakukan menggunakan *pipeline* yang memuat *preprocessing* dan model, kemudian kedua model divalidasi menggunakan GridSearchCV dengan 5-fold cross-validation untuk mencari kombinasi hyperparameter terbaik. *Random Forest* dilatih dengan membangun banyak *decision tree* lalu menggabungkan hasil *voting*, sedangkan *Logistic Regression* mencari koefisien terbaik untuk memisahkan kelas. Hasil validasi menunjukkan *Random Forest* dengan parameter terbaik (n_estimators=200, max_depth=10, min_samples_split=5) memperoleh akurasi 0.8049 dan AUC 0.5116, sementara *Logistic Regression* dengan parameter terbaik (C=0.1, penalty=L1) menghasilkan akurasi 0.5226 dan AUC 0.5050.

4.5. Hasil Evaluasi

1. ***Confusion Matrix*:**
   - ***Random Forest*:**
     Hasil pengujian model *Random Forest* dalam mendeteksi transaksi *fraud* ditunjukkan pada Tabel 4, yang menampilkan distribusi prediksi antara kelas *fraud* dan *non-fraud* berdasarkan *confusion matrix*.

Table 3. *Confusion Matrix* Model *Random Forest*

	Prediksi *Fraud* (1)	**Prediksi *Non-Fraud* (0)**
***Fraud* (1)**	31815	6167
***Non-Fraud* (0)**	1638	380

   - ***Logistic Regression*:**
     Tabel 5 menunjukkan hasil pengujian model *Logistic Regression* dalam mendeteksi transaksi fraud, yang menampilkan distribusi prediksi antara kelas *fraud* dan *non-fraud* berdasarkan *confusion matrix*.

Table 4. *Confusion Matrix* Model *Logistic Regression*

	Prediksi *Fraud* (1)	**Prediksi *Non-Fraud* (0)**
***Fraud* (1)**	19949	18033
***Non-Fraud* (0)**	1061	957

2. **Metrik Evaluasi**:
   Hasil evaluasi menunjukkan kinerja dua algoritma dalam mendeteksi transaksi *fraud* pada layanan keuangan digital.
   - ***Random Forest***
     - *Accuracy*: 0.8049
     - *Precision*: 0.0580

- *Recall*: 0.1883
- *F-1 Score*: 0.0887

- ***Logistic Regression***
  - *Accuracy*: 0.5226
  - *Precision*: 0.0504
  - *Recall*: 0.4742
  - *F-1 Score*: 0.0911

Dari hasil ini terlihat bahwa *Random Forest* memiliki *accuracy* yang lebih tinggi, tetapi kesulitan dalam mendeteksi transaksi *fraud* (kelas minoritas) seperti ditunjukkan oleh nilai *Precision*, *Recall*, dan F1-Score yang rendah. *Logistic Regression*, meskipun *accuracy* keseluruhannya lebih rendah, menunjukkan kemampuan *recall* yang sedikit lebih baik untuk kelas *fraud*. Hal ini menegaskan pentingnya penerapan teknik tambahan, seperti *oversampling* atau *cost-sensitive learning*, untuk menangani ketidakseimbangan data dan meningkatkan deteksi transaksi *fraud*.

3. **AUC**: Hasil evaluasi AUC menunjukkan kemampuan kedua model dalam membedakan transaksi *fraud* dan *non-fraud*.

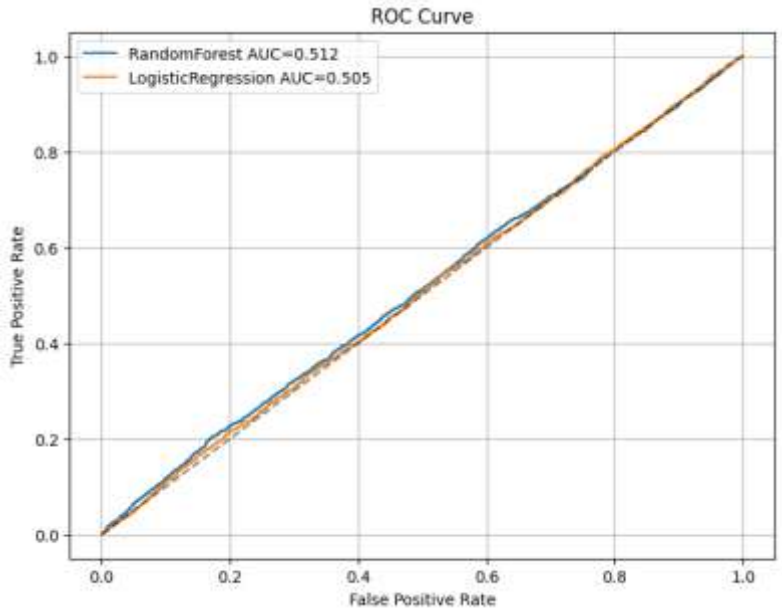
- ***Random Forest***:
  - AUC: 0.5116
- ***Logistic Regression***:
  - AUC: 0.5050

Nilai AUC yang rendah pada kedua model menunjukkan bahwa keduanya memiliki kemampuan yang terbatas dalam memisahkan kelas *fraud* dan *non-fraud*. Hal ini menegaskan perlunya penerapan teknik tambahan, seperti *oversampling*, *cost-sensitive learning*, atau penggunaan model *ensemble* lain, untuk meningkatkan kemampuan diskriminasi antara transaksi *fraud* dan *non-fraud*.

4.6. Grafik dan Visualisasi

4.6.1. Visualisasi ROC Curve

Untuk mengevaluasi kemampuan model dalam membedakan antara transaksi *fraud* dan *non-fraud*, digunakan ROC *Curve* (*Receiver Operating Characteristic*). Grafik ini menampilkan hubungan antara *True Positive Rate (Recall)* dan *False Positive Rate*, serta memberikan gambaran seberapa baik model mampu memisahkan kedua kelas. Berikut Gambar 2 menampilkan hasil visualisasi ROC *Curve*.



Gambar 2. ROC *Curve Comparison*.

Berdasarkan hasil evaluasi di atas, berikut adalah beberapa poin penting yang ditemukan:

1. **Kinerja Model**: Random Forest memiliki *Accuracy* 80,5% dan AUC 0,5116. *Precision* dan *Recall* untuk kelas *non-fraud* masing-masing 95,1% dan 83,8%, sedangkan untuk kelas *fraud* hanya 5,8% dan 18,8%, dengan F1-Score 8,87%. Hal ini menunjukkan bahwa meskipun akurasinya tinggi, model kurang mampu membedakan transaksi *fraud* dengan baik. *Logistic Regression* memiliki *Accuracy* 52,3% dan AUC 0,5050, dengan *precision* tinggi untuk kelas *non-fraud* (94,95%) tetapi *recall* rendah (52,5%), dan untuk kelas *fraud recall* 47,4% serta F1-Score 9,11%, menunjukkan performa yang juga kurang optimal dalam mendeteksi *fraud*.
2. ***Precision vs Recall***: *Random Forest* memiliki *precision* tinggi untuk kelas *non-fraud* (95,1%) dan *recall* 83,8%, namun untuk kelas *fraud precision* dan *recall* sangat rendah (5,8% dan 18,8%). *Logistic Regression* lebih seimbang antara keduanya, dengan *recall* untuk kelas *fraud* 47,4%, tetapi *accuracy* keseluruhan lebih rendah.
3. **AUC**: AUC untuk kedua model rendah, *Random Forest* 0,5116 dan *Logistic Regression* 0,5050, menunjukkan keduanya kesulitan membedakan antara *fraud* dan *non-fraud*.
4. **Ketidakseimbangan Data**: Ketidakseimbangan data menjadi tantangan utama. Meskipun dataset bisa diubah menjadi seimbang, dalam implementasi nyata pendekatan seperti ***cost-sensitive learning*** atau ***oversampling*** diperlukan untuk meningkatkan performa model dalam menangani data yang tidak seimbang.

Studi kasus ini menunjukkan bahwa penggunaan algoritma *data mining*, khususnya ***Random Forest***, dapat memberikan hasil yang baik dalam deteksi *fraud* pada layanan keuangan digital. Meskipun ***Logistic Regression*** lebih mudah diinterpretasikan, ***Random Forest*** memiliki akurasi yang lebih tinggi dan kemampuan untuk menangani data yang kompleks. Namun, ***Random Forest*** menunjukkan AUC yang rendah (0,5116), yang mengindikasikan keterbatasan dalam memisahkan kelas *fraud* dan *non-fraud*. Oleh karena itu, untuk implementasi yang lebih efektif, disarankan menggunakan teknik tambahan seperti ***cost-sensitive learning*** atau ***oversampling*** untuk menangani ketidakseimbangan data.

5. Kesimpulan

Pemanfaatan algoritma *data mining*, khususnya *Random Forest*, terbukti cukup efektif dalam mendeteksi transaksi *fraud* pada layanan keuangan digital. Dengan akurasi 80,5% dan *F1-Score* 8,87% untuk kelas *fraud*, model ini menunjukkan kemampuan terbatas dalam mengidentifikasi transaksi *fraud* secara tepat. Fitur-fitur seperti Nominal, Selisih Waktu, dan Jarak Lokasi Transaksi tetap berperan penting dalam mendeteksi pola transaksi *fraud*, di mana transaksi dengan nilai besar dan yang terjadi pada waktu atau lokasi yang tidak biasa sering menjadi indikator dari aktivitas *fraud*.

Precision untuk kelas fraud hanya 5,8% dan recall 18,8%, sehingga *Random Forest* cenderung menghasilkan banyak transaksi fraud yang terlewat, meskipun precision untuk kelas non-fraud tinggi (95,1%). AUC model 0,5116 menegaskan keterbatasan dalam membedakan kelas fraud dan non-fraud. Oleh karena itu, disarankan untuk menggunakan model tambahan atau teknik lain seperti *AdaBoost*, *XGBoost*, *cost-sensitive learning*, atau *oversampling* untuk meningkatkan kemampuan diskriminasi antara transaksi *fraud* dan *non-fraud*. Fokus utama dalam pengawasan transaksi mencurigakan dapat membantu mengurangi risiko kerugian secara signifikan dan meningkatkan kepercayaan pelanggan dalam sistem keuangan digital.

References

[1] N. Setiawan and I. Wahyudi, "Pencegahan fraud pada kejahatan siber perbankan," *Kabillah: Journal of Social Community*, vol. 8, no. 1, pp. 508–518, 2023.

[2] Otoritas Jasa Keuangan (OJK), "Panduan Strategi Anti Fraud Strategi Anti Fraud Penyelenggara Inovasi Teknologi Sektor Keuangan (ITSK)," 2024. [Online]. Available: https://www.ojk.go.id/id/Publikasi/Roadmap-dan-Pedoman/ITSK/Documents/PANDUAN%20STRATEGI%20ANTI%20FRAUD%20%28ITSK%29%202024.pdf?utm_source=chatgpt.com

[3] Satuan Tugas Pemberantasan Aktivitas Keuangan Ilegal (Satgas PASTI), "Waspada Penipuan Website Mengatasnamakan Indonesia Anti-Scam Centre (IASC)," 2025. Accessed: Nov. 17, 2025. [Online]. Available: https://ojk.go.id/id/berita-dan-kegiatan/info-terkini/Documents/Pages/Waspada-Penipuan-Website-Mengatasnamakan-Indonesia-Anti-Scam-Centre-IASC/Satgas%20PASTI%20-%20Waspada%20Penipuan%20Website%20Mengatasnamakan%20Indonesia%20Anti-Scam%20Centre%20(IASC).pdf

[4] M. Sánchez-Aguayo, L. Urquiza-Aguiar, and J. Estrada-Jiménez, "Fraud detection using the fraud triangle theory and data mining techniques: A literature review," *Computers*, vol. 10, no. 10, p. 121, 2021.

[5] A. Misrina, A. B. Pramesti, D. S. Salsabillah, A. M. Muliawati, and D. M. Putri, "Peranan Audit Berbasis IT dalam Mendeteksi Indikasi Fraud pada Era Transformasi Digital," in *Prosiding National Seminar on Accounting, Finance, and Economics (NSAFE)*, 2021.

[6] L. Gaswira and T. Meutia, "Pengaruh Penerapan Big Data Analisis Dalam Pendeteksian Fraud: Literature Review," *Jurnal Riset Akuntansi*, vol. 2, no. 2, pp. 111–120, 2024.

[7] A. G. Pratama, "Integrasi Teknik Data Mining Dalam Sistem Pemantauan Keamanan Cyber," *Jurnal Dunia Data*, vol. 1, no. 6, 2024.

[8] Z. Zhang, J. Li, C. Liu, and X. Wang, "Random Forest Algorithm for Fraud Detection," *Journal of Machine Learning Research*, vol. 15, no. 3, pp. 456–470, 2020.

[9] R. Ardhitha, R. Anugerah, and T. Sutabri, "Analisis Penerapan Machine Learning dan Algoritma Anomali untuk Deteksi Penipuan pada Transaksi Digital," *Repeater: Publikasi Teknik Informatika dan Jaringan*, vol. 3, no. 1, pp. 80–90, 2025.

[10] I. Gede Iwan Sudipa *et al.*, *Data Mining*. PT Global Eksekutif Teknologi, 2023. [Online]. Available: www.globaleksekutifteknologi.co.id

[11] R. Fitriana, A. N. Habyba, and E. Febriani, *Data Mining dan Aplikasinya: Contoh Kasus di industri manufaktur dan jasa*. wawasan Ilmu, 2022.

[12] S. H. Ali and A. T. Raslan, "Using Data Mining Techniques for Fraud Detection in The Non-banking Sector," *Journal of Computing and Communication*, vol. 3, no. 1, pp. 132–142, 2024.

[13] Z. Hamid, F. Khalique, S. Mahmood, A. Daud, A. Bukhari, and B. Alshemaimri, "Healthcare insurance fraud detection using data mining," *BMC Med Inform Decis Mak*, vol. 24, no. 1, p. 112, 2024.

[14] H. Susana, "Penerapan Model Klasifikasi Metode Naive Bayes Terhadap Penggunaan Akses Internet," *Jurnal Riset Sistem Informasi Dan Teknologi Informasi (JURSISTEKNI)*, vol. 4, no. 1, pp. 1–8, 2022.

[15] S. M. Natzir, "Perbandingan Kinerja Model Pembelajaran Mesin dalam Prediksi Banjir menggunakan KNN, Naive Bayes, dan Random Forest," *HOAQ (High Education of Organization Archive Quality): Jurnal Teknologi Informasi*, vol. 14, no. 2, pp. 59–64, 2023.

[16] H. A. Salman, A. Kalakech, and A. Steiti, "Random forest algorithm overview," *Babylonian Journal of Machine Learning*, vol. 2024, pp. 69–79, 2024.

[17] F. R. Valerian, M. Syarief, and D. A. Fatah, "Klasifikasi tingkat obesitas menggunakan metode gbm dan confusion matrix," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 9, no. 2, pp. 2242–2249, 2025.

[18] S. Usman and F. Aziz, "Analisis Perilaku Pelanggan menggunakan Metode Ensemble Logistic Regression," *Jurnal Teknologi Dan Ilmu Komputer Prima (Jutikomp)*, vol. 6, no. 2, pp. 90–97, 2023.

[19] A. D. Putri, F. Sholekhah, E. Dadynata, L. Efrizoni, R. Rahmaddeni, and N. Sapina, "Penerapan Algoritma Decesion Tree C4. 5 untuk Memprediksi Tingkat Kelangsungan Hidup Pasien Kanker Tiroid: The Application of C4. 5 Decision Tree Algorithm for Predicting the Survival Rate of Thyroid Cancer Patients," *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 4, no. 4, pp. 1485–1495, 2024.