

Analisis pola *Fraud* pada *Payment Gateway* Berbasis *Unsupervised Learning* Menggunakan *Isolation Forest*

Haikal Ikhwan

Universitas Muhammadiyah Sumatera Utara, Indonesia

Email: haikalmedan2003@gmail.com

ABSTRAK

Perkembangan teknologi digital yang pesat telah mendorong peningkatan transaksi online melalui *Payment Gateway*. Namun, hal ini juga diiringi dengan meningkatnya kasus penipuan (*Fraud*) yang merugikan merchant dan konsumen. Penelitian ini bertujuan untuk mengembangkan sistem deteksi *Fraud* pada *Payment Gateway* menggunakan metode *Unsupervised Learning* dengan algoritma *Isolation Forest*. Dataset yang digunakan merupakan dataset transaksi kartu kredit yang diperoleh dari Kaggle, yang terdiri dari 284.807 transaksi dengan komposisi 0,17% *Fraud*. Selain itu, untuk keperluan validasi, digunakan juga data sandbox dari Midtrans sebanyak 500 transaksi. Model *Isolation Forest* dilatih dengan pendekatan data balancing dan hyperparameter tuning. Hasil pengujian menunjukkan bahwa model mencapai akurasi sebesar 43,81%, precision 27,83%, dan recall 78,32%. Meskipun precision masih rendah, recall yang tinggi mengindikasikan bahwa model mampu mendeteksi sebagian besar transaksi *Fraud*. Sistem diimplementasikan dalam bentuk aplikasi web berbasis Laravel yang terintegrasi dengan Flask API untuk deteksi *Fraud* secara real-time, serta dilengkapi dengan dashboard admin untuk monitoring transaksi dan status *Fraud*. Penelitian ini memberikan kontribusi berupa sistem deteksi *Fraud* yang dapat membantu merchant dalam mengidentifikasi transaksi mencurigakan secara otomatis, serta menjadi dasar pengembangan sistem keamanan yang lebih baik di masa depan.

Kata Kunci: *Fraud Detection*; *Payment Gateway*; *Isolation Forest*.

ABSTRACT

The rapid development of digital technology has driven an increase in online transactions through *Payment Gateways*. However, this is also accompanied by a rise in *Fraud* cases that harm both merchants and consumers. This research aims to develop a *Fraud Detection* system on *Payment Gateways* using *Unsupervised Learning* with the *Isolation Forest* algorithm. The dataset used is a credit card transaction dataset obtained from Kaggle, consisting of 284,807 transactions with a *Fraud* composition of 0.17%. Additionally, for validation purposes, 500 transactions from the Midtrans sandbox were also used. The *Isolation Forest* model was trained using a data balancing approach and hyperparameter tuning. The test results show that the model achieves an accuracy of 43.81%, precision of 27.83%, and recall of 78.32%. Although precision is still low, the high recall indicates that the model is capable of detecting most *Fraudulent* transactions. The system is implemented as a Laravel-based web application integrated with a Flask API for real-time *Fraud Detection*, equipped with an admin dashboard for transaction monitoring and *Fraud* status. This research contributes a *Fraud Detection* system that can assist merchants in automatically identifying suspicious transactions and serves as a foundation for developing better security systems in the future.

Keywords: *Fraud Detection*; *Payment Gateway*; *Isolation Forest*.

PENDAHULUAN

Perkembangan teknologi dan informasi selama beberapa tahun belakangan ini membuat perubahan yang cukup pesat pada beberapa sektor, di antaranya pada sektor perbankan (Hasyim et al. 2023). Inovasi *Financial Technology* (FinTech) telah membawa perubahan besar pada sektor keuangan dengan mempermudah berbagai mekanisme transaksi, khususnya melalui sistem pembayaran digital. Mengingat pesatnya penyebaran internet serta penggunaan *smartphone* di tanah air, masyarakat kini cenderung memilih metode pembayaran non-tunai sebagai kebutuhan utama. Hal ini didorong oleh aspek efisiensi, kecepatan, dan perlindungan keamanan yang ditawarkan, sehingga menjadikannya pilihan utama dalam aktivitas harian. Secara teknis, pembayaran digital diartikan sebagai proses transaksi elektronik yang mengintegrasikan teknologi untuk pengelolaan serta penerimaan data pembayaran (Puspitasari 2025). Tren ini sekaligus mengkonfirmasi bahwa arah perkembangan pemenuhan kebutuhan finansial di masa depan akan didominasi oleh transaksi tanpa uang tunai (*cashless*) serta pemanfaatan akun virtual berbasis FinTech (Al-Khowarizmi et al. 2022).

Menurut Bank Indonesia (2023), nilai transaksi digital banking tercatat Rp 58.478,24 triliun. Diantara bentuk implementasi transaksi elektronik yang banyak digunakan adalah layanan *Payment Gateway*. Menurut Siahaan and Sianturi (2024) *Payment Gateway* adalah teknologi yang mengelola pertukaran data pembayaran antara pembeli, penjual, dan pihak bank. Selain memfasilitasi kebutuhan transaksi rutin, sistem ini juga memastikan setiap pembayaran telah

.Peneliti seperti Thar and Wai (2024) menekankan bahwa *Fraud* digital memiliki karakteristik unik karena bergantung pada transaksi elektronik yang cepat, bervolume tinggi, serta sifatnya yang lintas batas, sehingga membuat metode proteksi konvensional mulai kehilangan relevansinya. Terlebih lagi, skema kecurangan ini tidak bersifat statis, melainkan terus berevolusi secara dinamis mengikuti setiap celah keamanan yang ditemukan pada ekosistem transaksi elektronik. Hasil penelitian dari George et al. (2023) mengungkapkan bahwa metode *supervised learning*, seperti *decision trees*, *logistic regression*, dan *support vector machines*, tetap menjadi pilihan utama karena kinerjanya yang stabil serta mudah dipahami. Namun, untuk menghadapi pola *Fraud* yang terus berevolusi pada data yang sangat tidak seimbang, pendekatan *Unsupervised Learning* kini semakin sering diandalkan sebagai solusi mencari pola Anomali yang lebih adaptif.

Berdasarkan permasalahan *Fraud* digital, salah satunya terkait transaksi *Fraud* pada *Payment Gateway*, Kennedy et al. (2022) berpendapat bahwa pendekatan *Unsupervised Learning* menjadi alternatif yang relevan. Alasan utamanya adalah metode ini mampu bekerja secara optimal meskipun harus menghadapi dataset yang sangat tidak seimbang. Selain itu, keunggulan utamanya terletak pada kemampuan sistem untuk mengenali pola *Fraud* tanpa bergantung pada label data. Salah satu algoritma *Unsupervised Learning* yang banyak digunakan ialah *Isolation Forest*. Dalam studinya, Karczmarek et al. (2021) menyebutkan bahwa *Isolation Forest* menjadi pilihan

populer untuk mencari pola Anomali karena prinsip kerjanya yang mengandalkan konsep jarak dan kepadatan data. Metode ini bekerja dengan cara yang cukup sederhana, yaitu membangun hutan pohon biner dari sampel data acak. Pada praktiknya, status sebuah transaksi dianggap Anomali berdasarkan seberapa cepat data tersebut terisolasi di dalam struktur pohon atau jumlah node yang dilewatinya. Meski dikenal sangat cepat dan efisien dalam memproses data, algoritma ini unik karena strukturnya cenderung tetap konsisten dan tidak banyak mengalami perubahan teknis sejak pertama kali diperkenalkan. Dalam penelitian Prasad et al. (2025) menunjukkan bahwa efektivitas sistem dalam mengenali transaksi ilegal dapat ditingkatkan secara drastis dengan mengintegrasikan *Isolation Forest* ke dalam analisis penyimpangan statis. Keunggulan utama dari metode yang diusulkan ini adalah kemampuannya mendeteksi *Fraud* dengan akurasi tinggi tanpa memicu banyak kesalahan deteksi (positif palsu). Hal inilah yang menjadikan pendekatan tersebut sangat relevan untuk menjaga keamanan pada layanan *Payment Gateway*.

Meskipun studi terdahulu telah banyak mengeksplorasi deteksi *Fraud* menggunakan metode supervised (Thar & Wai 2024) maupun pendekatan hybrid (Prasad et al. 2025) literatur yang secara spesifik mengkaji penerapan *Unsupervised Learning* melalui algoritma *Isolation Forest* pada sistem *Payment Gateway* masih sangat terbatas. Terlebih lagi, integrasi deteksi Anomali dalam arsitektur sistem secara end-to-end belum banyak dibahas secara mendalam. Guna mengisi celah tersebut, penelitian ini mengembangkan sistem *Payment Gateway* menggunakan framework Laravel yang terintegrasi dengan modul deteksi *Fraud* berbasis Python. Pemilihan judul “Analisis Pola *Fraud* pada *Payment Gateway* Berbasis *Unsupervised Learning* Menggunakan *Isolation Forest*” didasarkan pada kebutuhan akan sistem keamanan yang adaptif terhadap dinamika transaksi digital di Indonesia. Penelitian ini diharapkan dapat memberikan kontribusi nyata berupa rancangan arsitektur sistem yang komprehensif serta evaluasi efektivitas algoritma dalam mendeteksi Anomali pada data yang tidak berlabel.

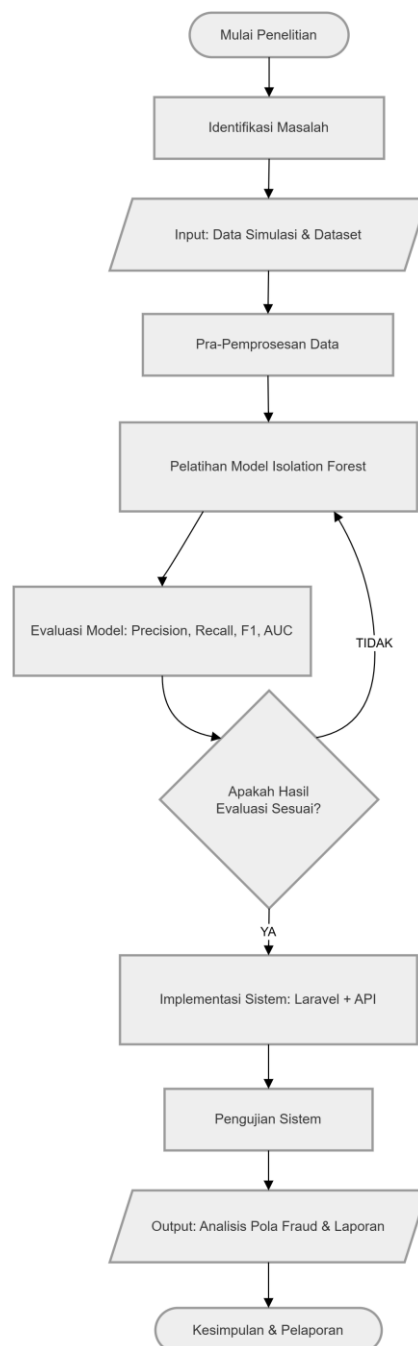
METODE PENELITIAN

Desain Penelitian

Penelitian ini menggunakan pendekatan kuantitatif berjenis eksperimen terapan dengan iterasi bertahap. Strategi pengembangan sistem menggunakan pendekatan *Minimum Viable Product* (MVP), yakni membangun versi paling sederhana dari *Payment Gateway* yang berfungsi sebagai fungsi inti. Konsep MVP menekankan pembuatan produk minimal yang memungkinkan pengujian validasi fungsi inti dengan usaha minimal. Tahap awal merancang *Payment Gateway* sederhana (misalnya backend Laravel dan integrasi Midtrans Sandbox) agar alur transaksi dasar berjalan: pengguna memilih produk, diarahkan ke halaman pembayaran eksternal, dan proses pembayaran selesai (simulasi). Tahap selanjutnya mengumpulkan data transaksi dari sistem simulasi tersebut sebagai data eksperimen primer. Selanjutnya, model deteksi *Fraud* (*Isolation Forest*) dikembangkan secara terpisah (menggunakan

dataset publik berlabel *Fraud/non- Fraud*) lalu diintegrasikan ke backend melalui API (Flask/FastAPI). Akhirnya, sistem diuji dan dievaluasi secara menyeluruh. Dengan desain iteratif ini, setiap tahap (dari fungsi dasar hingga modul analisis *Fraud*) dapat diuji dan diperbaiki secara sistematis sebelum melanjutkan ke tahap berikutnya.

Flowchart pada Gambar 1 menunjukkan alur tahapan penelitian dalam pengembangan sistem *Payment Gateway* berbasis deteksi *Fraud* menggunakan algoritma *Isolation Forest*, mulai dari identifikasi masalah hingga kesimpulan penelitian. Berikut gambar flowchart tahapan penelitian:



Gambar 1 Flowchart Tahapan Penelitian

Data penelitian terdiri atas data transaksi dari dataset publik dan data transaksi simulasi yang dihasilkan melalui sistem yang dikembangkan. Dataset *creditcard.csv* berisi 284.807 transaksi, sedangkan *transactions.csv* berisi 2.501 transaksi simulasi. Data transaksi simulasi digunakan untuk mendukung pengujian sistem, sedangkan dataset publik digunakan dalam proses eksperimen model sesuai dengan konfigurasi penelitian.

Sebelum digunakan, data diperiksa untuk mengidentifikasi nilai kosong, duplikasi, perbedaan format, serta ketidaksesuaian tipe data. Selanjutnya, fitur transaksi disiapkan agar dapat diproses oleh algoritma. Setelah tahap *feature engineering* dan standardisasi, hasil eksperimen mencatat 199.364 data untuk pelatihan dan 85.443 data untuk pengujian.

Dalam penelitian ini, keluaran model diperlakukan sebagai indikasi anomali, bukan sebagai bukti bahwa suatu transaksi merupakan tindak penipuan yang telah terkonfirmasi. Label yang tersedia pada dataset digunakan untuk mengevaluasi hasil deteksi terhadap data pengujian.

Prapemrosesan Data

Prapemrosesan dilakukan untuk memastikan bahwa data transaksi memiliki format yang sesuai dengan kebutuhan model. Tahapan ini mencakup pemeriksaan nilai kosong, identifikasi data duplikat, penyesuaian tipe data, transformasi fitur kategorikal yang diperlukan, serta standardisasi fitur numerik.

Fitur yang digunakan untuk prediksi disiapkan dalam format numerik. Pada implementasi layanan deteksi, model menerima 13 fitur numerik yang diekstraksi dari parameter transaksi. Fitur tersebut kemudian diproses menggunakan transformasi yang sesuai dengan konfigurasi model sebelum tahap prediksi dilakukan.

Tahap prapemrosesan perlu diterapkan secara konsisten pada data pelatihan, data pengujian, dan data baru yang dikirim melalui API. Konsistensi tersebut diperlukan agar representasi fitur pada saat prediksi sesuai dengan representasi yang digunakan saat pelatihan model.

Penerapan Algoritma *Isolation Forest*

Algoritma *Isolation Forest* digunakan untuk mengidentifikasi transaksi yang memiliki karakteristik berbeda dari sebagian besar data. Algoritma ini bekerja dengan membangun kumpulan pohon isolasi yang memisahkan sampel berdasarkan pemilihan fitur dan titik pemisah secara acak. Sampel yang lebih mudah diisolasi cenderung memperoleh skor anomali yang berbeda dibandingkan sampel yang berada dalam pola mayoritas.

Implementasi model menggunakan pustaka *scikit-learn* pada lingkungan Python. Parameter yang berkaitan dengan proses pelatihan meliputi *n_estimators*, *max_samples*, dan *contamination*. Parameter tersebut memengaruhi jumlah pohon, jumlah sampel yang digunakan pada setiap pohon, serta perkiraan proporsi anomali

dalam data. Konfigurasi eksperimen yang digunakan harus merujuk pada parameter aktual dari model yang menghasilkan hasil evaluasi penelitian.

Setelah model dilatih, setiap transaksi yang diuji memperoleh hasil prediksi dan skor anomali. Pada implementasi sistem, keluaran tersebut dikonversi menjadi status yang dapat dibaca oleh aplikasi. Transaksi yang memenuhi kriteria anomali ditandai sebagai transaksi terindikasi *Fraud*, sedangkan transaksi lainnya ditandai sebagai normal. Penandaan tersebut digunakan untuk mendukung pemantauan dan pemeriksaan lanjutan oleh administrator.

Evaluasi Model

Evaluasi dilakukan menggunakan data pengujian dan metrik *precision*, *recall*, *F1-score*, *accuracy*, serta *ROC-AUC*. Metrik tersebut digunakan untuk menggambarkan ketepatan prediksi, kemampuan menemukan data berlabel positif, keseimbangan antara *precision* dan *recall*, proporsi prediksi yang benar, serta kemampuan pemisahan skor antara kelas yang dievaluasi.

Precision mengukur proporsi prediksi positif yang benar, sedangkan *recall* mengukur proporsi data positif yang berhasil terdeteksi. *F1-score* merupakan rata-rata harmonik *precision* dan *recall*. *Accuracy* menunjukkan proporsi seluruh prediksi yang benar, sedangkan *ROC-AUC* mengevaluasi kemampuan pemisahan kelas berdasarkan berbagai ambang skor.

Walaupun *Isolation Forest* merupakan algoritma *Unsupervised Learning*, metrik berbasis label tetap dapat digunakan untuk mengevaluasi hasilnya apabila label pembandingan tersedia. Dalam konteks penelitian ini, label pada dataset digunakan sebagai acuan evaluasi, bukan sebagai label yang harus diberikan kepada model selama proses pembelajaran tanpa pengawasan. Oleh karena itu, hasil metrik perlu ditafsirkan bersama distribusi kelas dan matriks kebingungan agar tidak hanya bergantung pada nilai *accuracy* atau *ROC-AUC*.

Integrasi Model dengan Sistem Payment Gateway

Aplikasi transaksi dibangun menggunakan Laravel dan terhubung dengan Midtrans Sandbox untuk mensimulasikan proses pembayaran. Modul deteksi anomali dibangun menggunakan Python dan disediakan melalui Flask REST API. Ketika data transaksi perlu dianalisis, aplikasi Laravel mengirimkan parameter yang diperlukan melalui permintaan HTTP dengan metode POST.

Layanan Flask menerima permintaan, memeriksa parameter, menyiapkan fitur numerik, menjalankan transformasi data, dan meneruskan fitur tersebut ke model *Isolation Forest*. Hasil prediksi kemudian dikirim kembali dalam format JSON yang memuat informasi seperti skor anomali, indikator prediksi, tingkat keyakinan yang ditampilkan sistem, dan status transaksi sesuai implementasi.

Laravel menggunakan respons tersebut untuk menampilkan hasil analisis dan menyimpan atau menyajikan informasi transaksi pada dashboard administrator.

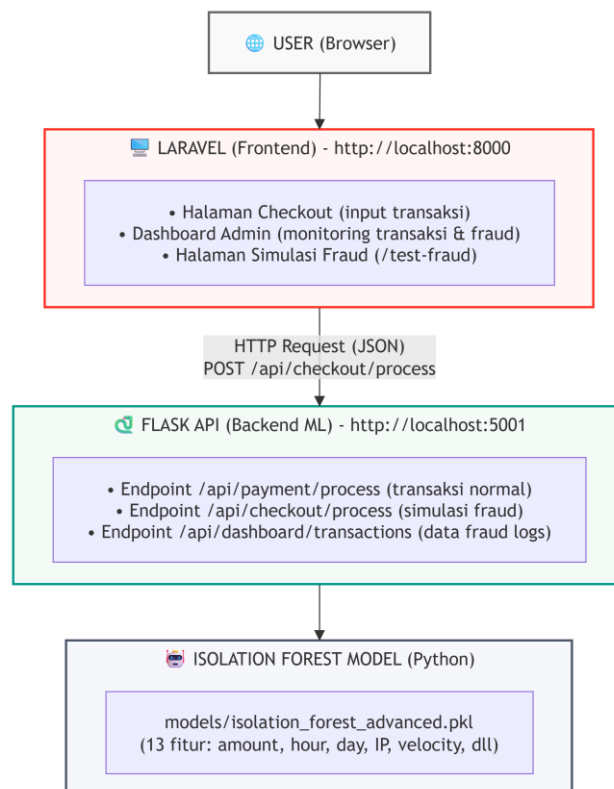
Integrasi ini memungkinkan proses deteksi dilakukan melalui layanan terpisah tanpa mengharuskan model Python dijalankan langsung di dalam aplikasi Laravel.

HASIL DAN PEMBAHASAN

Implementasi Sistem *Payment Gateway*

Sistem yang dikembangkan mengintegrasikan aplikasi Laravel, layanan pembayaran Midtrans Sandbox, dan layanan deteksi anomali berbasis Flask. Pengguna dapat memilih produk, mengisi data transaksi, dan melanjutkan proses pembayaran pada lingkungan simulasi. Penggunaan sandbox memungkinkan alur pembayaran diuji tanpa memproses pembayaran riil.

Pada sisi aplikasi, status pembayaran ditangani oleh mekanisme integrasi yang tersedia, termasuk penerimaan notifikasi dari layanan pembayaran. Sementara itu, modul deteksi anomali bertugas menganalisis karakteristik transaksi dan menghasilkan indikasi berdasarkan pola yang dipelajari model. Kedua fungsi tersebut memiliki peran yang berbeda: status pembayaran menjelaskan keadaan proses pembayaran, sedangkan status anomali menunjukkan hasil analisis karakteristik transaksi.



Gambar 2 Arsitektur Sistem

Gambar tersebut memperlihatkan hubungan antarbagian sistem secara ringkas. Laravel berperan sebagai aplikasi utama, Midtrans Sandbox menyimulasikan proses pembayaran, Flask menyediakan antarmuka prediksi, dan *Isolation Forest* melakukan

analisis anomali. Hasil prediksi diteruskan kembali ke aplikasi untuk ditampilkan dan dipantau.



Checkout ×

Mobile Legends

344 Diamonds

Rp 147.000

ID Player *

20023812

Nama *

haikal ikhwan

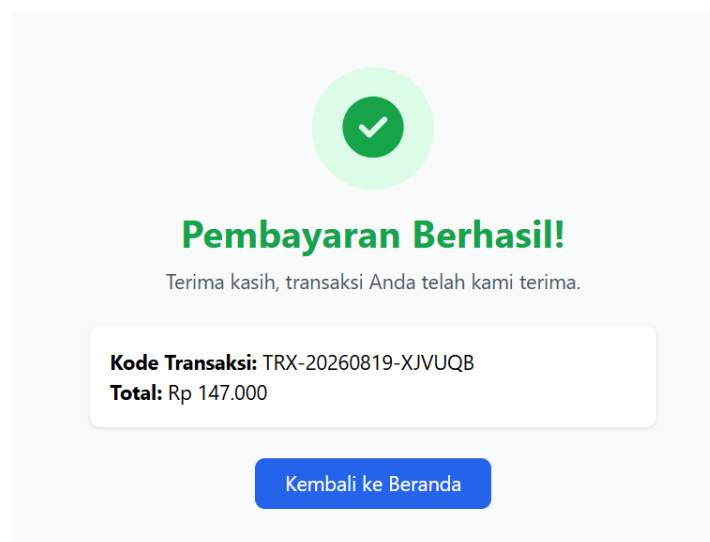
Email *

haikalmedan2003@gmail.com

Batal Bayar

Gambar 3 Pop-up Form Input Data Checkout

Antarmuka checkout digunakan sebagai bukti bahwa sistem transaksi telah diimplementasikan kemudian sistem menampilkan konfirmasi bahwa pembayaran berhasil beserta kode transaksi dan total pembayaran.

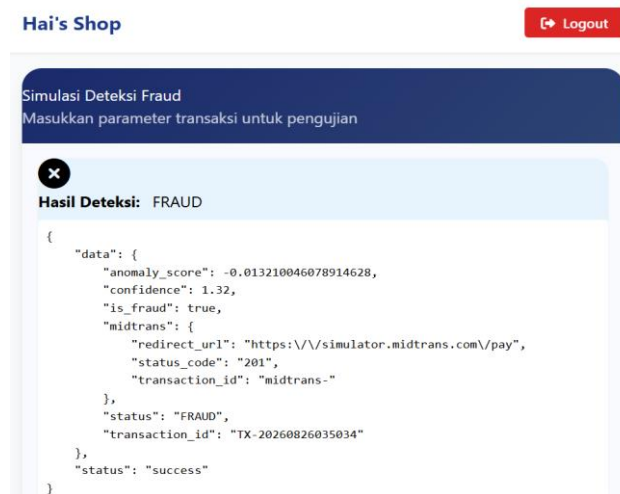


Gambar 4 Tampilan Notifikasi Pembayaran Berhasil

Implementasi Deteksi Anomali

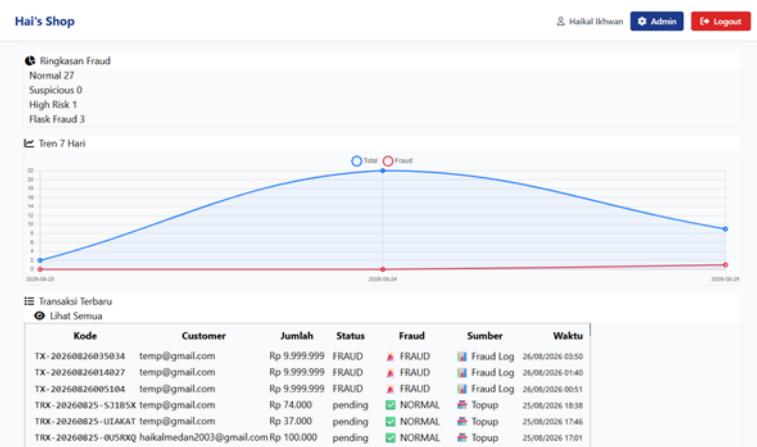
Pengujian deteksi dilakukan melalui halaman simulasi yang memungkinkan parameter transaksi dimasukkan untuk dianalisis oleh model. Salah satu skenario menggunakan nominal transaksi Rp9.999.999, waktu transaksi pukul 23.00, hari ke-6 sesuai representasi pada sistem, serta metode pembayaran yang tercatat sebagai unknown.

Pada skenario tersebut, layanan API mengembalikan skor anomali sebesar -0,01321 dan indikator *is_Fraud* bernilai true. Hasil tersebut menunjukkan bahwa transaksi pada skenario uji diklasifikasikan oleh model sebagai anomali berdasarkan ambang keputusan yang diterapkan pada implementasi.



Gambar 5 Respons API dan Hasil Prediksi Fraud

Hasil pengujian tersebut memperlihatkan bahwa parameter transaksi dapat dikirim ke layanan deteksi dan hasil prediksi dapat dikembalikan ke aplikasi. Namun, satu skenario pengujian belum cukup untuk membuktikan bahwa seluruh transaksi mencurigakan dapat dideteksi secara konsisten. Hasil tersebut perlu dipahami sebagai bukti fungsional integrasi pada skenario yang diuji, sedangkan kemampuan deteksi model secara keseluruhan dibahas melalui metrik evaluasi.



Gambar 6 Tampilan Dashboard Ringkasan dan Analisis Tren Fraud.

Implementasi Dashboard Monitoring

Dashboard administrator menyediakan ringkasan status transaksi, informasi transaksi terbaru, dan fasilitas pemantauan. Berdasarkan hasil pengujian antarmuka yang tercatat, dashboard menampilkan 27 transaksi berstatus normal, 1 transaksi berstatus High Risk, dan 3 transaksi yang ditandai sebagai *Fraud* oleh Flask. Sistem juga menyediakan pencarian transaksi, penyaringan berdasarkan status, serta fasilitas ekspor data ke format CSV.

Dashboard membantu administrator meninjau hasil prediksi dalam konteks operasional sistem. Fitur pencarian dan penyaringan memudahkan penelusuran transaksi, sedangkan ekspor CSV mendukung penyimpanan dan pemeriksaan data lebih lanjut. Angka pada dashboard merupakan ringkasan dari data yang tampil pada saat pengujian dan tidak dapat dianggap sebagai ukuran performa model pada keseluruhan dataset.

Hasil Evaluasi Model

Evaluasi model dilakukan pada data pengujian yang dilaporkan berjumlah 85.443 transaksi. Ringkasan metrik yang tercatat pada hasil eksperimen ditampilkan pada Tabel berikut.

Tabel 1 Hasil Evaluasi Model *Isolation Forest*

Metrik	Kelas Normal	Kelas <i>Fraud</i>	Rata-rata
Precision	1,00	0,08	—
Recall	0,98	0,96	—
F1-score	0,99	0,15	—
Accuracy	—	—	0,98
Macro F1-score	—	—	0,57
Weighted F1-score	—	—	0,99
ROC-AUC	—	—	0,9979*

Keterangan: nilai ROC-AUC mengikuti angka pada tabel hasil penelitian yang tersedia dan perlu diverifikasi terhadap keluaran evaluasi asli.

Hasil tersebut menunjukkan adanya perbedaan antara kemampuan model mengenali kelas normal dan kelas *Fraud*. Nilai precision untuk kelas normal sebesar 1,00, sedangkan precision kelas *Fraud* sebesar 0,08. Artinya, berdasarkan hasil evaluasi tersebut, hanya sebagian kecil dari seluruh prediksi *Fraud* yang sesuai dengan label positif pada data pembandingan.

Di sisi lain, recall kelas *Fraud* sebesar 0,96 menunjukkan bahwa sebagian besar data yang berlabel *Fraud* berhasil terdeteksi oleh model pada pengujian tersebut. Akan tetapi, tingginya recall tidak secara otomatis berarti bahwa seluruh prediksi positif akurat. Nilai F1-score kelas *Fraud* sebesar 0,15 memperlihatkan bahwa keseimbangan antara precision dan recall pada kelas tersebut masih terbatas.

Perbedaan ini penting dalam penerapan deteksi anomali pada transaksi digital. Sistem yang berorientasi pada penemuan sebanyak mungkin transaksi berisiko dapat

menghasilkan lebih banyak peringatan yang ternyata bukan positif menurut label pembanding. Oleh karena itu, hasil prediksi sebaiknya digunakan sebagai sinyal untuk pemeriksaan lanjutan, bukan sebagai keputusan final bahwa transaksi merupakan tindak penipuan.

Nilai accuracy sebesar 0,98 dan weighted F1-score sebesar 0,99 perlu ditafsirkan dengan mempertimbangkan ketidakseimbangan jumlah sampel antarkelas. Dalam dataset yang didominasi transaksi normal, metrik agregat dapat terlihat tinggi walaupun performa prediksi pada kelas minoritas masih terbatas. Oleh sebab itu, precision, recall, F1-score kelas *Fraud*, dan matriks kebingungan tetap perlu menjadi bagian utama pembahasan.

Analisis Confusion Matrix

Matriks kebingungan yang tercatat pada hasil penelitian menunjukkan jumlah prediksi berikut.

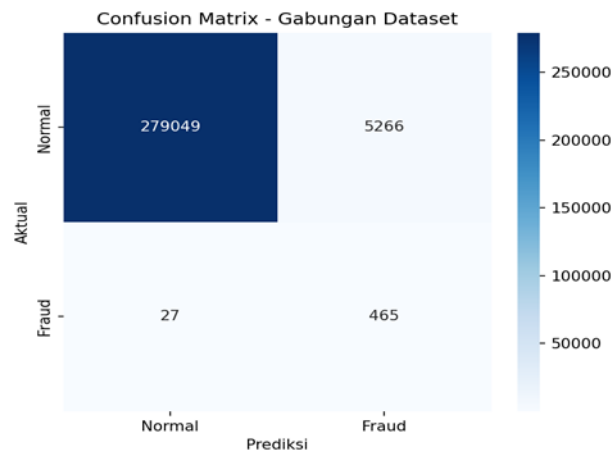
Tabel 2 Confusion Matrix pada Data Pengujian

Kelas aktual	Prediksi Normal	Prediksi <i>Fraud</i>
Normal	83.694	1.601
<i>Fraud</i>	6	142

Berdasarkan matriks tersebut, sebanyak 83.694 transaksi normal diklasifikasikan sebagai normal, sedangkan 1.601 transaksi normal diklasifikasikan sebagai *Fraud*. Selain itu, sebanyak 142 transaksi berlabel *Fraud* berhasil terdeteksi dan 6 transaksi berlabel *Fraud* diklasifikasikan sebagai normal.

Jumlah 1.601 transaksi normal yang diprediksi sebagai *Fraud* menunjukkan adanya positif palsu (false positive) yang perlu diperhatikan. Dalam penerapan operasional, kondisi ini berpotensi menambah beban pemeriksaan administrator apabila setiap prediksi positif harus ditinjau secara manual. Sementara itu, terdapat 6 transaksi berlabel *Fraud* yang tidak terdeteksi pada pengujian tersebut, sehingga sistem masih memiliki kemungkinan melewatkan sebagian transaksi positif.

Temuan ini memperlihatkan adanya pertukaran antara kemampuan menemukan transaksi berlabel *Fraud* dan ketepatan setiap peringatan yang dihasilkan. Penentuan ambang keputusan perlu mempertimbangkan kedua aspek tersebut, terutama apabila sistem digunakan untuk membantu pemantauan transaksi dalam jumlah besar.



Gambar 7 Confusion Matrix (Gabungan Dataset)

Visualisasi matriks kebingungan dapat membantu pembaca melihat perbandingan prediksi pada masing-masing kelas. Gambar harus menggunakan nilai yang sama dengan tabel agar tidak menimbulkan perbedaan hasil pelaporan.

Analisis ROC-AUC dan Skor Anomali

Nilai ROC-AUC pada tabel hasil penelitian tercatat sebesar 0,9979. Secara umum, ROC-AUC menggambarkan kemampuan skor model dalam membedakan kelas positif dan negatif pada berbagai ambang keputusan. Namun, nilai tersebut perlu ditafsirkan sesuai cara perhitungan yang digunakan, terutama karena *Isolation Forest* menghasilkan skor anomali dan bukan probabilitas kelas secara langsung.

Sebelum nilai ROC-AUC dicantumkan sebagai hasil akhir, perhitungan perlu diperiksa kembali dengan memastikan bahwa skor yang digunakan, arah skor anomali, label pembanding, dan data pengujian sudah sesuai. Nilai ROC-AUC juga perlu diseragamkan karena terdapat perbedaan angka pada bagian lain naskah penelitian.

Skor anomali pada pengujian sistem menunjukkan bagaimana model memberikan keluaran yang dapat digunakan untuk membedakan pola transaksi. Sebagai contoh, skor -0,01321 pada salah satu skenario menghasilkan indikator anomali. Nilai skor tersebut tidak sebaiknya ditafsirkan sebagai probabilitas penipuan sebesar persentase tertentu, kecuali telah dilakukan kalibrasi probabilitas yang sesuai. Demikian pula, nilai confidence yang ditampilkan oleh antarmuka perlu dijelaskan cara perhitungannya sebelum ditafsirkan sebagai tingkat keyakinan statistik model.

Pengujian Integrasi Laravel dan Flask

Pengujian integrasi dilakukan untuk memastikan bahwa aplikasi Laravel dapat mengirimkan parameter transaksi ke layanan Flask dan menerima hasil prediksi. Alur pengujian dimulai dari pengiriman permintaan POST, penerimaan parameter oleh API, pemrosesan fitur, prediksi menggunakan *Isolation Forest*, dan pengembalian hasil dalam format JSON.

Hasil pengujian mencatat bahwa layanan API dapat mengembalikan indikator prediksi beserta skor anomali. Pada salah satu pengujian, sistem juga menghasilkan ID transaksi dan kode respons HTTP 201. Temuan tersebut mendukung bahwa alur permintaan dan respons dapat dijalankan pada skenario yang diuji.

Keberhasilan integrasi perlu dibedakan dari keberhasilan deteksi. Respons API yang berhasil menunjukkan bahwa komunikasi antarlayanan berjalan, tetapi tidak dengan sendirinya membuktikan bahwa prediksi model akurat. Ketepatan prediksi tetap perlu dinilai berdasarkan hasil evaluasi model, sedangkan kestabilan integrasi perlu diuji melalui berbagai kondisi, termasuk parameter tidak lengkap, format data yang tidak sesuai, dan kegagalan layanan.

Pengujian Skenario Transaksi

Pengujian skenario dilakukan untuk mengamati respons sistem pada karakteristik transaksi yang berbeda. Pada contoh transaksi normal yang tercatat, nominal transaksi adalah Rp147.000, waktu transaksi pukul 14.00, hari ke-3 pada representasi sistem, dan metode pembayaran kartu kredit. Sistem menghasilkan skor anomali sebesar +0,044, indikator *is_Fraud* bernilai false, status NORMAL, serta nilai confidence yang ditampilkan sebesar 85,5%.

Pada skenario lain, transaksi dengan nominal Rp9.999.999, waktu transaksi pukul 23.00, hari ke-6, dan metode pembayaran unknown menghasilkan skor anomali -0,01321 dengan indikator *is_Fraud* bernilai true.

Perbedaan keluaran pada dua skenario tersebut menunjukkan bahwa sistem dapat memberikan status yang berbeda untuk masukan transaksi yang berbeda. Meskipun demikian, kedua contoh tersebut bersifat ilustratif dan tidak dapat digunakan sendirian untuk menyimpulkan tingkat akurasi model. Pengujian yang lebih luas diperlukan untuk menilai kestabilan hasil pada variasi nominal, waktu transaksi, metode pembayaran, serta kombinasi fitur lainnya.

Hasil penelitian menunjukkan bahwa algoritma *Isolation Forest* dapat diintegrasikan dengan sistem transaksi berbasis Laravel melalui layanan Flask API. Integrasi ini memungkinkan karakteristik transaksi dianalisis oleh model Python dan hasilnya disajikan kembali melalui aplikasi utama. Dashboard juga menyediakan sarana untuk meninjau status transaksi, melakukan pencarian, menyaring data, dan mengekspor laporan.

Pada aspek evaluasi, nilai recall kelas *Fraud* yang tercatat sebesar 0,96 menunjukkan kemampuan menemukan sebagian besar data berlabel positif pada data pengujian. Namun, nilai precision sebesar 0,08 dan F1-score sebesar 0,15 menunjukkan bahwa banyak prediksi positif tidak sesuai dengan label pembandingan. Dengan demikian, evaluasi tidak cukup hanya menekankan kemampuan model mendeteksi anomali; ketepatan peringatan juga perlu diperhatikan.

Hasil tersebut menegaskan bahwa sistem yang dikembangkan lebih tepat diposisikan sebagai alat bantu pemantauan transaksi yang berpotensi anomali. Keputusan mengenai validitas transaksi tetap memerlukan pemeriksaan lanjutan dan

informasi pendukung lainnya. Pendekatan ini juga sesuai dengan karakteristik deteksi anomali, karena transaksi yang berbeda dari pola mayoritas belum tentu merupakan penipuan.

Terdapat beberapa keterbatasan yang perlu diperhatikan. Data simulasi dan dataset publik dapat memiliki karakteristik yang berbeda dari transaksi pada lingkungan operasional sesungguhnya. Selain itu, ketidakseimbangan kelas dapat memengaruhi interpretasi metrik agregat. Kinerja model juga bergantung pada pemilihan fitur, konfigurasi parameter, standarisasi, dan ambang keputusan yang diterapkan. Oleh karena itu, penelitian lanjutan perlu memeriksa konsistensi proses eksperimen, melakukan pengujian tambahan, dan mengevaluasi dampak positif palsu terhadap alur pemeriksaan transaksi.

KESIMPULAN

Penelitian ini menerapkan algoritma *Isolation Forest* untuk menganalisis pola transaksi yang terindikasi anomali pada sistem *Payment Gateway* berbasis Laravel. Model dikembangkan menggunakan Python dan diintegrasikan melalui Flask REST API, sedangkan Midtrans Sandbox digunakan untuk menyimulasikan proses pembayaran. Hasil implementasi menunjukkan bahwa aplikasi dapat mengirimkan parameter transaksi ke layanan deteksi dan menerima keluaran prediksi untuk ditampilkan pada sistem monitoring.

Berdasarkan hasil evaluasi yang tercatat, model memperoleh recall kelas *Fraud* sebesar 0,96, precision sebesar 0,08, dan F1-score sebesar 0,15. Hasil tersebut menunjukkan bahwa sebagian besar data berlabel *Fraud* pada pengujian berhasil terdeteksi, tetapi prediksi positif masih memiliki tingkat ketepatan yang terbatas. Nilai accuracy dan ROC-AUC perlu ditafsirkan bersama metrik kelas minoritas serta diverifikasi kembali terhadap keluaran eksperimen asli.

Dengan demikian, penerapan *Isolation Forest* pada sistem yang dikembangkan dapat mendukung proses pemantauan transaksi yang memiliki karakteristik tidak biasa. Namun, hasil model sebaiknya diperlakukan sebagai indikasi anomali yang memerlukan pemeriksaan lanjutan, bukan sebagai penetapan final bahwa transaksi merupakan tindak penipuan.

DAFTAR PUSTAKA

- Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial *Fraud Detection* Based on Machine Learning: A Systematic Literature Review. In *Applied Sciences (Switzerland)* (Vol. 12, Number 19). MDPI. <https://doi.org/10.3390/app12199637>
- Al-Khowarizmi, A., Syah, R., & Elveny, M. (2022). The model of business intelligence development by applying cooperative society based financial technology. In X. S. Yang, S. Sherratt, N. Dey, & A. Joshi (Eds.), *Proceedings of Sixth International Congress on Information and Communication Technology* (Vol. 235, pp. 117–125). Springer. https://doi.org/10.1007/978-981-16-2377-6_13

- Apruzzese, G., Laskov, P., Montes De Oca, E., Mallouli, W., Brdalo Rapa, L., Grammatopoulos, A. V., & Di Franco, F. (2023). The Role of Machine Learning in Cybersecurity. *Digital Threats: Research and Practice*, 4(1). <https://doi.org/10.1145/3545574>
- Ardhi Baskara, A., Maharani Piranti, N., Fahrury Romdendine Manajemen Teknologi Keimigrasian, M., Imigrasi Jalan Raya Gandul No, P., & Depok, K. (2025). FRAMEWORK DATA MINING : SEBUAH SURVEI. In *Jurnal Mahasiswa Teknik Informatika* (Vol. 9, Number 3).
- Bank Indonesia. (2024, January 17). BI catat nilai transaksi digital banking 2023 Rp 58.478,24 triliun. *PPID Provinsi Kalimantan Timur*. <https://ppid-dev.kaltimprov.go.id/post/bi-catat-nilai-transaksi-digital-banking-2023-rp-58-478-24-triliun>
- BCBS. (2023). *Basel Committee on Banking Supervision Discussion paper Digital Fraud and banking: supervisory and financial stability implications*. www.bis.org
- Bodepudi, H. (2021). Credit Card Fraud Detection Using Unsupervised Machine Learning Algorithms. *International Journal of Computer Trends and Technology*, 69(8), 1–3. <https://doi.org/10.14445/22312803/IJCTT-V69I8P101>
- Diva, M., & Anshori, I. (2024). Penggunaan E-Wallet Sebagai Inovasi Transaksi Digital: *Literatur Review*. 2(6). <https://journal.institercom-edu.org/index.php/multiple>
- FutureCISO. (2025). Rising scam threats in Indonesia's real-time payments ecosystem. <https://futureciso.tech/rising-scam-threats-in-indonesias-real-time-payments-ecosystem/>
- George, M. Z. H., Alam, M. K., & Hasan, M. T. (2023). MACHINE LEARNING FOR FRAUD DETECTION IN DIGITAL BANKING: A SYSTEMATIC LITERATURE REVIEW. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 03(01), 37–61. <https://doi.org/10.63125/913ksy63>
- Harlan, H. (2026). Sinergi : Jurnal Ilmiah Multidisiplin Penipuan dalam Ekosistem Digital Finance: Kajian Teoritis dan Strategi Mitigasi di Indonesia. *Jurnal Ilmiah Multidisiplin*. <https://publikasi.ahlalkamal.com/index.php/sinergi>
- Hasyim, Pulungan, F. A., Sitorus, H. N. S., & Muliana, R. S. (2023). Increasing the Use of Electronic Money Transactions (E-Money) in Indonesian Society. *Indonesian Journal of Accounting and Financial Technology*, 1(2), 59–70. <https://doi.org/10.55927/crypto.v1i2.4267>
- Karczmarek, P., Kiersztyn, A., Pedrycz, W., & Al-Enezi, J. R. (2021). Generalized Isolation Forest for anomaly Detection. *Applied Soft Computing*, 107, Article 107354. <https://doi.org/10.1016/j.asoc.2021.107354>
- Kennedy, K., Mac Namee, B., & Delany, S. J. (2022). A novel approach for Unsupervised Learning of highly-imbalanced data. In *Proceedings of the 2022 IEEE 5th International Conference on Cognitive Machine Intelligence (CogMI)* (pp. 10–18). <https://doi.org/10.1109/CogMI56440.2022.00018>

- Lesouple, J., Baudoin, C., Spigai, M., & Tourneret, J.-Y. (2021). *Pattern Recognition Letters Generalized Isolation Forest for Anomaly Detection*. <https://www.sciencedirect.com/science/article/pii/S0167865521002063>
- Nursansiwati, D. A., & Armiani, A. (2022). Peran Strategi Bisnis Fintech *Payment Gateway* dalam Meningkatkan Kinerja UMKM di NTB. *Owner*, 7(1), 367–378. <https://doi.org/10.33395/owner.v7i1.1219>
- Parmar, P. P., & Sheth, K. P. (n.d.). *Peer-Reviewed, Multidisciplinary & Multilingual Journal DIGITAL FINANCIAL TRANSACTION USAGE AND DEMOGRAPHICS OF CUSTOMERS: EVIDENCE FROM GUJARAT*. Retrieved <http://vidyajournal.org>
- Prasad, K. A., Pattabirani, G., & Sundaramoorthy, K. (2025). *Insights into Anomaly Detection: A Survey and Comparative Analysis of Techniques for Time Series Data from Industrial Environment* (pp. 871–907). https://doi.org/10.2991/978-94-6463-662-8_71
- Pratiwi, A. A., Aulia, N., Nikmah, N., Indriani, D., Audy, K., Studi, P., & Syariah, E. (2026). Perkembangan dan Implementasi Digital Payment dalam Mendukung Sistem Pembayaran Cashless di Indonesia. *Jurnal Ekonomi Manajemen Dan Bisnis*, 3, 343–352. <https://doi.org/10.62017/jemb>
- Puspitasari, A. (2025). Transformation of the Financial Sector and Digital Payments in Indonesia. *ORGANIZE: Journal of Economics, Management and Finance*, 4(2), 145–154. <https://doi.org/10.58355/organize.v4i2.122>
- Shaveta. (2023). A review on machine learning. *International Journal of Science and Research Archive*, 9(1), 281–285. <https://doi.org/10.30574/ijrsra.2023.9.1.0410>
- Siahaan, R. A., Sianturi, R. A., & Korespondensi, P. (2024). ANALISIS PERBANDINGAN PAYMENT GATEWAY UNTUK SISTEM PEMBAYARAN BERBASIS APLIKASI DENGAN COMPARATIVE STUDY. 11(2), 291–296. <https://doi.org/10.25126/jtiik.2024117680>
- Thar, K. W., & Wai, T. T. (2024). Machine learning based predictive modelling for *Fraud Detection* in digital banking. In *Proceedings of the 2024 IEEE Conference on Computer Applications (ICCA)* (pp. 1–5). <https://doi.org/10.1109/ICCA62361.2024.10532788>
- Zanah, A. S., Calista, B., Dewi, W. N., & Sokibi, P. (2025). Deteksi Dini *Fraud* pada Layanan Keuangan Digital Menggunakan Metode Random Forest. In *Indonesian Journal on Data Science* (Vol. 3, Number 2). <https://ejournal.unjaya.ac.id/index.php/ijds>