Jurnal Teknologi dan Bisnis
https://journal.stmiki.ac.id
E-ISSN: XXXX-XXXX | P-ISSN: XXXX-XXXX
Vol. 1 No. 1 (2027) | Januari
OPEN ACCESS
https://doi.org/10.63447/jtb.v1i1.2264

Pengembangan Model Agentic AI untuk Deteksi Fraud dan Penilaian Risiko Transaksi pada Ekosistem Pembayaran Digital di Indonesia

Ismail [1*], Syarifuddin [2]

[1*, 2] Program Studi Manajemen Informatika, STMIK Indonesia Banda Aceh, Kota Banda Aceh, Provinsi Aceh, Indonesia

Email: ismail@stmiki.ac.id [1*], syarifuddin@stmiki.ac.id [2]

Histori Artikel:
Dikirim 16 November 2026; *Diterima dalam bentuk revisi* 21 November 2026; *Diterima* 30 November 2026; *Diterbitkan* 28 Januari 2027. Semua hak dilindungi oleh Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) STMIK Indonesia Banda Aceh.

Abstrak

Perkembangan pembayaran digital di Indonesia meningkatkan kemudahan transaksi sekaligus menghadirkan risiko fraud yang semakin kompleks dan dinamis. Sistem deteksi berbasis aturan dan model klasifikasi konvensional masih memiliki keterbatasan dalam memahami konteks transaksi serta menghasilkan keputusan risiko secara adaptif. Penelitian ini bertujuan mengembangkan model Agentic Artificial Intelligence (Agentic AI) untuk mendeteksi fraud dan melakukan penilaian risiko transaksi pada ekosistem pembayaran digital di Indonesia. Penelitian menggunakan pendekatan kuantitatif eksperimental melalui tahapan pengumpulan data, data preprocessing, feature engineering, deteksi fraud, agentic risk assessment, risk scoring, pengujian, dan evaluasi model. Dataset terdiri atas 20.000 transaksi dengan 18.000 transaksi normal dan 2.000 transaksi fraud. Model dibandingkan menggunakan beberapa algoritma machine learning, kemudian diintegrasikan dengan mekanisme Agentic AI untuk menghasilkan klasifikasi risiko dan rekomendasi tindakan. Hasil eksperimen menunjukkan bahwa model Agentic AI menghasilkan accuracy 98,3%, precision 94,1%, recall 93,2%, F1-score 93,6%, dan AUC 0,98. Model juga mampu mengelompokkan transaksi ke dalam kategori risiko rendah, sedang, dan tinggi serta memberikan rekomendasi tindakan berupa approve, additional verification, dan flag for investigation. Hasil penelitian menunjukkan bahwa integrasi Agentic AI dapat memberikan pendekatan yang lebih adaptif dan komprehensif dalam mendukung deteksi fraud serta penilaian risiko transaksi digital.

Kata kunci: Agentic AI, fraud detection, risk assessment, digital payment, FinTech, machine learning.

Abstract

The growth of digital payments in Indonesia has enhanced transaction convenience while simultaneously introducing increasingly complex and dynamic fraud risks. Rule-based detection systems and conventional classification models remain limited in their ability to comprehend transaction contexts and generate adaptive risk decisions. This study aims to develop an Agentic Artificial Intelligence (Agentic AI) model to detect fraud and assess transaction risks within Indonesia's digital payment ecosystem. The research employs an experimental quantitative approach comprising data collection, preprocessing, feature engineering, fraud detection, agentic risk assessment, risk scoring, testing, and model evaluation. The dataset consists of 20,000 transactions, comprising 18,000 legitimate and 2,000 fraudulent transactions. The model was compared against various machine learning algorithms and subsequently integrated with an Agentic AI mechanism to generate risk classifications and action recommendations. Experimental results demonstrate that the Agentic AI model achieved an accuracy of 98.3%, precision of 94.1%, recall of 93.2%, F1-score of 93.6%, and an AUC of 0.98. The model is capable of categorizing transactions into low, medium, and high-risk levels and providing action recommendations—specifically: approve, additional verification, or flag for investigation. The findings indicate that integrating Agentic AI offers a more adaptive and comprehensive approach to supporting fraud detection and risk assessment in digital transactions.

Keywords: Agentic AI, fraud detection, risk assessment, digital payment, FinTech, machine learning.

Jurnal Teknologi dan Bisnis
https://journal.stmiki.ac.id
E-ISSN: XXXX-XXXX | P-ISSN: XXXX-XXXX
Vol. 1 No. 1 (2027) | Januari
OPEN ACCESS
https://doi.org/10.63447/jtb.v1i1.2264

1. Pendahuluan

Perkembangan teknologi finansial (financial technology/FinTech) telah mendorong perubahan signifikan dalam ekosistem pembayaran di Indonesia. Transformasi tersebut ditandai dengan semakin luasnya penggunaan pembayaran digital melalui mobile banking, dompet digital, QR payment, internet banking, dan berbagai platform pembayaran elektronik (Qur'anisa, et al., 2024). Digitalisasi memberikan kemudahan, kecepatan, dan efisiensi dalam melakukan transaksi keuangan, tetapi pada saat yang sama juga memperluas permukaan risiko terhadap berbagai bentuk kejahatan finansial. Peningkatan volume transaksi, keberagaman kanal pembayaran, serta karakteristik transaksi yang berlangsung secara real-time menyebabkan proses identifikasi transaksi mencurigakan menjadi semakin kompleks (Afifah, et al., 2025). Fraud dalam ekosistem pembayaran digital dapat terjadi melalui berbagai pola, seperti transaksi tidak sah, pengambilalihan akun, pencurian identitas, manipulasi transaksi, penyalahgunaan instrumen pembayaran, hingga pola transaksi yang sengaja dirancang untuk menghindari sistem pengawasan (Tarigan, 2025). Permasalahan tersebut menjadi semakin kompleks karena pola fraud dapat berubah dengan cepat mengikuti perkembangan teknologi dan perilaku pelaku. Transaksi yang pada satu kondisi terlihat normal dapat menjadi indikasi fraud apabila dikaitkan dengan lokasi, waktu, frekuensi, nilai transaksi, perangkat yang digunakan, atau hubungan dengan transaksi lainnya. Oleh karena itu, sistem keamanan pembayaran digital tidak cukup hanya mengandalkan aturan statis (rule-based system), tetapi membutuhkan pendekatan analitik yang mampu mempelajari pola, beradaptasi terhadap perubahan, dan memberikan penilaian risiko secara dinamis (Saputra, et al., 2026).

Artificial Intelligence (AI) dan machine learning telah banyak digunakan untuk mendukung proses deteksi fraud dengan memanfaatkan karakteristik transaksi sebagai masukan untuk mengidentifikasi pola transaksi normal dan anomaly (Ilahi & Budiono, 2024). Pendekatan seperti decision tree, random forest, support vector machine, neural network, dan deep learning dapat digunakan untuk melakukan klasifikasi maupun prediksi terhadap transaksi berisiko (Sidik, et al., 2026). Meskipun demikian, sebagian besar pendekatan tersebut masih berorientasi pada fungsi prediktif, yaitu menghasilkan klasifikasi atau skor risiko berdasarkan data yang diberikan. Sistem tersebut belum sepenuhnya mampu menjalankan rangkaian proses secara adaptif, seperti mengidentifikasi pola baru, menggabungkan berbagai sumber informasi, melakukan evaluasi terhadap hasil analisis, serta menentukan tindakan lanjutan berdasarkan konteks Risiko (Riyanto, et al., 2026). Perkembangan Agentic AI menawarkan paradigma baru dalam penerapan kecerdasan buatan pada bidang keuangan. Berbeda dengan model AI konvensional yang umumnya menjalankan tugas prediksi berdasarkan instruksi dan data tertentu, Agentic AI dirancang untuk menjalankan serangkaian proses secara lebih otonom melalui kemampuan memahami tujuan, melakukan analisis, menggunakan berbagai sumber informasi, mengevaluasi hasil, dan menentukan tindakan berdasarkan aturan atau tujuan yang telah ditetapkan (Mutaqin, et al., 2025). Dalam konteks pembayaran digital, pendekatan ini berpotensi digunakan untuk membangun sistem yang tidak hanya mendeteksi indikasi fraud, tetapi juga melakukan penilaian tingkat risiko transaksi secara dinamis berdasarkan berbagai atribut dan konteks transaksi (Ismanda, et al., 2025).

Penerapan Agentic AI dalam deteksi fraud juga memungkinkan terbentuknya mekanisme analisis berlapis. Agen AI dapat melakukan pemeriksaan karakteristik transaksi, membandingkan transaksi dengan pola historis, mengidentifikasi anomali, menghitung tingkat risiko, dan menghasilkan rekomendasi tindakan seperti transaksi normal, transaksi memerlukan verifikasi tambahan, atau transaksi berisiko tinggi untuk dilakukan pemeriksaan lebih lanjut (Iskandar, et al., 2025). Pendekatan tersebut dapat meningkatkan kemampuan sistem dalam menghadapi pola fraud yang bersifat dinamis sekaligus mengurangi ketergantungan terhadap aturan deteksi yang harus diperbarui secara manual. Meskipun penelitian mengenai deteksi fraud berbasis machine learning dan deep learning telah berkembang cukup pesat, penelitian yang secara khusus mengintegrasikan konsep Agentic AI dengan fraud detection dan transaction risk assessment dalam konteks ekosistem pembayaran digital Indonesia masih memiliki ruang pengembangan (Widjaja, 2025). Salah satu tantangan utama adalah bagaimana merancang mekanisme agen yang mampu menggabungkan

Jurnal Teknologi dan Bisnis
https://journal.stmiki.ac.id
E-ISSN: XXXX-XXXX | P-ISSN: XXXX-XXXX
Vol. 1 No. 1 (2027) | Januari
OPEN ACCESS
https://doi.org/10.63447/jtb.v1i1.2264

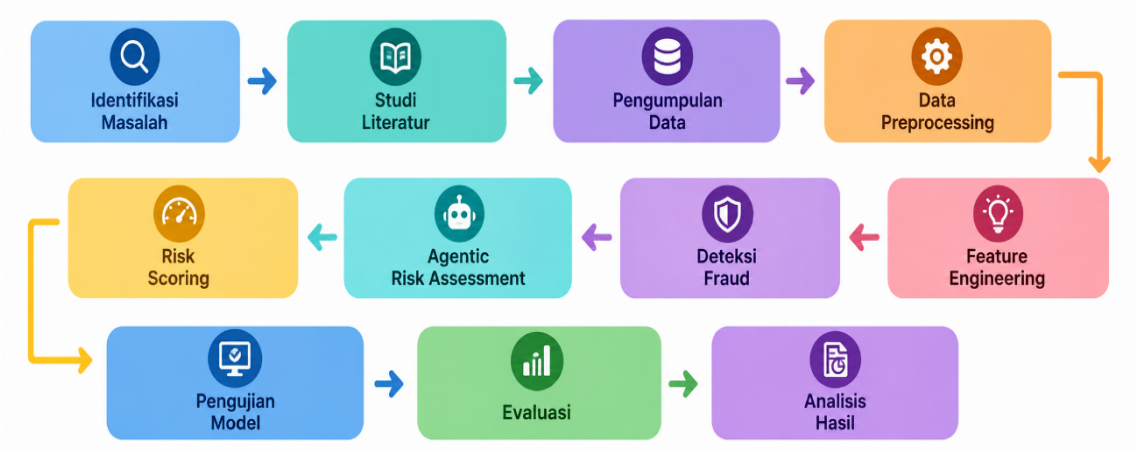
hasil deteksi anomali dengan penilaian risiko secara kontekstual, tetap dapat dijelaskan kepada pengguna, serta menghasilkan keputusan yang konsisten. Selain itu, sistem juga perlu mempertimbangkan karakteristik data transaksi yang tidak seimbang (imbalanced data), karena jumlah transaksi normal umumnya jauh lebih besar dibandingkan transaksi fraud (Ardhitha, et al., 2025).

Berdasarkan permasalahan tersebut, penelitian ini mengusulkan pengembangan model Agentic AI untuk deteksi fraud dan penilaian risiko transaksi pada ekosistem pembayaran digital di Indonesia. Model yang dikembangkan diarahkan untuk mengintegrasikan analisis karakteristik transaksi, deteksi anomali, risk scoring, dan mekanisme pengambilan keputusan berbasis agen. Sistem akan mengevaluasi sejumlah atribut transaksi untuk menghasilkan klasifikasi fraud serta tingkat risiko transaksi. Selanjutnya, performa model akan dievaluasi menggunakan metrik yang relevan, seperti accuracy, precision, recall, F1-score, dan AUC-ROC, dengan perhatian khusus terhadap kemampuan model dalam mendeteksi transaksi fraud yang jumlahnya relatif kecil dibandingkan transaksi normal. Penelitian ini diharapkan memberikan kontribusi dalam pengembangan pendekatan kecerdasan buatan yang lebih adaptif untuk keamanan pembayaran digital. Dari sisi akademik, penelitian ini memperluas penerapan Agentic AI dalam bidang FinTech, khususnya pada integrasi deteksi fraud dan penilaian risiko transaksi. Dari sisi praktis, model yang dihasilkan diharapkan dapat menjadi dasar pengembangan sistem intelligent fraud monitoring yang mampu membantu penyedia layanan pembayaran dalam melakukan identifikasi transaksi berisiko secara lebih cepat, adaptif, dan berbasis data. Dengan demikian, penelitian ini tidak hanya berfokus pada kemampuan model dalam mendeteksi fraud, tetapi juga pada kemampuan membangun mekanisme analisis risiko yang dapat mendukung keamanan dan keandalan ekosistem pembayaran digital di Indonesia.

2. Metode Penelitian

2.1 Desain Penelitian

Penelitian ini menggunakan pendekatan kuantitatif eksperimental dengan tujuan mengembangkan dan mengevaluasi model Agentic Artificial Intelligence (Agentic AI) untuk mendeteksi transaksi fraud sekaligus melakukan penilaian tingkat risiko transaksi pada ekosistem pembayaran digital (Anggraini & Fatihaturrizqi, 2025). Penelitian dilakukan melalui beberapa tahapan utama, yaitu pengumpulan data, data preprocessing, eksplorasi data, rekayasa fitur (feature engineering), pembangunan model deteksi fraud, pengembangan mekanisme agentic decision, penilaian risiko transaksi, serta evaluasi kinerja model (Verawati, et al., 2026). Secara umum, alur penelitian dapat digambarkan sebagai berikut:



Gambar 1. Alur Penelitian

Jurnal Teknologi dan Bisnis
https://journal.stmiki.ac.id
E-ISSN: XXXX-XXXX | P-ISSN: XXXX-XXXX
Vol. 1 No. 1 (2027) | Januari
OPEN ACCESS
https://doi.org/10.63447/jtb.v1i1.2264

2.2 Data Penelitian

Data yang digunakan berupa data transaksi pembayaran digital yang memiliki karakteristik transaksi normal dan transaksi fraud. Data transaksi terdiri atas sejumlah atribut yang menggambarkan karakteristik aktivitas pembayaran, seperti:

Tabel 1. Data Transaksi Pembayaran Digital

Variabel	Keterangan
Transaction_ID	Identitas unik transaksi
Transaction_Amount	Nilai transaksi
Transaction_Time	Waktu transaksi
Transaction_Type	Jenis transaksi
Account_Age	Usia akun
Transaction_Frequency	Frekuensi transaksi
Device_Type	Jenis perangkat
Location	Lokasi transaksi
IP_Risk	Tingkat risiko alamat IP
Previous_Fraud	Riwayat fraud
Merchant_Category	Kategori merchant
Transaction_Distance	Jarak transaksi dari lokasi sebelumnya
Failed_Attempts	Jumlah percobaan transaksi gagal
Fraud_Label	Label transaksi normal/fraud

Variabel Fraud_Label digunakan sebagai variabel target dalam proses klasifikasi (Ramadhani, T., et al., 2025). Nilai 0 menunjukkan transaksi normal, sedangkan nilai 1 menunjukkan transaksi fraud. Untuk kebutuhan eksperimen, dataset dapat disusun dalam bentuk data yang memiliki karakteristik menyerupai transaksi pembayaran digital di Indonesia (Ramadhan, et al., 2026). Penggunaan data memungkinkan penelitian menguji mekanisme model tanpa menggunakan data pribadi atau data transaksi nasabah yang bersifat sensitif.

2.3 Data Preprocessing

Tahap preprocessing dilakukan untuk memastikan data dapat digunakan oleh model secara konsisten. Tahapan yang dilakukan meliputi:

1) pemeriksaan data kosong (missing value);
2) penghapusan data duplikat;
3) pemeriksaan nilai ekstrem (outlier);
4) transformasi data kategorikal;
5) normalisasi variabel numerik;
6) pemeriksaan ketidakseimbangan kelas (class imbalance); dan
7) pembagian dataset menjadi data pelatihan dan data pengujian.

Karena data fraud pada umumnya memiliki jumlah yang jauh lebih sedikit dibandingkan transaksi normal, penelitian mempertimbangkan teknik penanganan class imbalance, seperti SMOTE (Synthetic Minority Oversampling Technique) atau penggunaan class weighting pada model klasifikasi.

2.4 Feature Engineering

Tahap feature engineering dilakukan untuk menghasilkan fitur yang dapat meningkatkan kemampuan model dalam mengenali pola transaksi mencurigakan. Beberapa fitur turunan yang digunakan antara lain:

1) Transaction Velocity, yaitu jumlah transaksi dalam periode tertentu;
2) Amount Deviation, yaitu penyimpangan nilai transaksi terhadap pola historis;
3) Location Deviation, yaitu perubahan lokasi transaksi yang tidak biasa;
4) Device Change, yaitu perubahan perangkat yang digunakan;

Jurnal Teknologi dan Bisnis
https://journal.stmiki.ac.id
E-ISSN: XXXX-XXXX | P-ISSN: XXXX-XXXX
Vol. 1 No. 1 (2027) | Januari
OPEN ACCESS
https://doi.org/10.63447/jtb.v1i1.2264

5) Time Anomaly, yaitu transaksi yang dilakukan pada waktu yang tidak biasa;
6) Frequency Anomaly, yaitu peningkatan frekuensi transaksi secara tidak normal; dan
7) Historical Risk, yaitu tingkat risiko berdasarkan riwayat transaksi sebelumnya.

Fitur-fitur tersebut kemudian digunakan sebagai input untuk model deteksi fraud dan modul penilaian risiko.

2.5 Pengembangan Model Deteksi Fraud

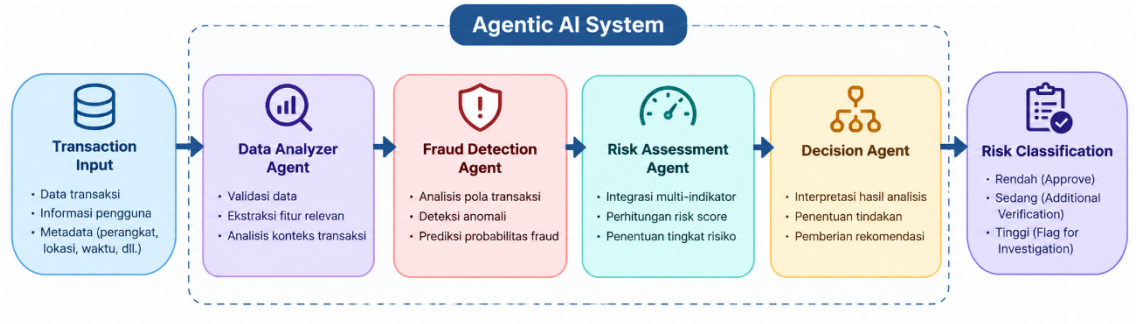
Pada tahap ini digunakan algoritma machine learning untuk mengidentifikasi apakah suatu transaksi termasuk transaksi normal atau fraud. Model utama dapat menggunakan Random Forest sebagai baseline model karena mampu menangani berbagai karakteristik data transaksi dan menghasilkan informasi mengenai kontribusi fitur terhadap keputusan klasifikasi. Sebagai pembanding, penelitian dapat menggunakan beberapa algoritma lain, seperti:

1) Logistic Regression;
2) Random Forest;
3) XGBoost; dan
4) Artificial Neural Network.

Perbandingan tersebut digunakan untuk mengetahui kemampuan masing-masing model sebelum hasilnya diintegrasikan ke dalam arsitektur Agentic AI.

2.6 Arsitektur Agentic AI

Komponen utama penelitian adalah pengembangan mekanisme Agentic AI yang bertindak sebagai lapisan analisis dan pengambilan keputusan di atas model deteksi fraud. Arsitektur yang digunakan terdiri atas beberapa komponen:



Gambar 2. Arsitektur Agentic AI

Setiap agen memiliki fungsi berbeda.

1) Data Analyzer Agent, bertugas menganalisis karakteristik transaksi, memeriksa kelengkapan data, dan mengidentifikasi fitur yang relevan.
2) Fraud Detection Agent, menggunakan model machine learning untuk menentukan probabilitas transaksi termasuk fraud.
3) Risk Assessment Agent, menggabungkan probabilitas fraud dengan faktor risiko lainnya untuk menghasilkan skor risiko transaksi.
4) Decision Agent, melakukan interpretasi terhadap skor risiko dan menentukan kategori tindakan yang sesuai.

2.7 Mekanisme Penilaian Risiko

Skor risiko transaksi dihitung berdasarkan kombinasi beberapa indikator. Secara konseptual, skor risiko dapat dirumuskan sebagai:

$$\text{RiskScore} = w_1F + w_2A + w_3L + w_4V + w_5H$$

Jurnal Teknologi dan Bisnis
https://journal.stmiki.ac.id
E-ISSN: XXXX-XXXX | P-ISSN: XXXX-XXXX
Vol. 1 No. 1 (2027) | Januari
OPEN ACCESS
https://doi.org/10.63447/jtb.v1i1.2264

Keterangan:

F	: probabilitas fraud;
A	: anomali nilai transaksi;
L	: anomali lokasi;
V	: anomali frekuensi/velocity;
H	: historical risk;
$w_1,\ldots,w_5$	:bobot masing-masing indikator.

Skor tersebut kemudian dikonversi menjadi tiga kategori:

Tabel 2. Skor Penilaian Risiko

Skor Risiko	Kategori	Interpretasi
0–30	Rendah	Transaksi relatif normal
31–70	Sedang	Membutuhkan pemeriksaan tambahan
71–100	Tinggi	Terindikasi memiliki risiko fraud tinggi

Batas kategori tersebut digunakan sebagai parameter eksperimen dan dapat disesuaikan berdasarkan hasil validasi model.

2.8 Mekanisme Pengambilan Keputusan Agent

Agent melakukan tindakan berdasarkan hasil risk scoring. Mekanisme keputusan dirancang sebagai berikut:

Risiko Rendah → Approve
Risiko Sedang → Additional Verification
Risiko Tinggi → Flag for Investigation

Dengan mekanisme tersebut, sistem tidak hanya menghasilkan label fraud/non-fraud, tetapi juga memberikan rekomendasi tindakan berdasarkan tingkat risiko.

2.9 Skenario Eksperimen

Penelitian menggunakan beberapa skenario eksperimen untuk mengetahui pengaruh integrasi Agentic AI terhadap kinerja sistem.

1) Skenario 1 Baseline, model machine learning digunakan secara langsung untuk klasifikasi fraud.
2) Skenario 2 Fraud Detection + Risk Scoring, model klasifikasi diintegrasikan dengan mekanisme penilaian risiko.
3) Skenario 3 Agentic AI, model klasifikasi, risk scoring, dan decision agent diintegrasikan menjadi satu arsitektur Agentic AI.

Hasil ketiga skenario dibandingkan untuk melihat perubahan kinerja dan kemampuan sistem dalam mengidentifikasi transaksi berisiko.

2.10 Evaluasi Model

Evaluasi dilakukan menggunakan beberapa metrik, yaitu:

1) $Accuracy = (TP + TN)/(TP + TN + FP + FN)$
2) $Precision = TP/(TP + FP)$
3) $Recall = TP/(TP + FN)$
4) $\mathrm{F1-Score} = 2 \times (Precision \times Recall)/(Precision + Recall)$

Selain itu digunakan AUC-ROC untuk mengevaluasi kemampuan model dalam membedakan transaksi normal dan fraud pada berbagai tingkat ambang klasifikasi. Untuk penelitian fraud detection, Recall dan F1-Score menjadi metrik penting karena model perlu mampu mendeteksi transaksi fraud tanpa hanya mengandalkan jumlah prediksi benar secara keseluruhan.

Jurnal Teknologi dan Bisnis
https://journal.stmiki.ac.id
E-ISSN: XXXX-XXXX | P-ISSN: XXXX-XXXX
Vol. 1 No. 1 (2027) | Januari
OPEN ACCESS
https://doi.org/10.63447/jtb.v1i1.2264

3. Hasil dan Pembahasan

3.1 Hasil

3.1.1 Karakteristik Dataset

Penelitian menggunakan dataset transaksi pembayaran digital sebanyak 20.000 transaksi. Dataset terdiri atas transaksi normal dan transaksi fraud dengan karakteristik transaksi pada ekosistem pembayaran digital.

Tabel 3. Transaksi Pembayaran Digital

Kategori	Jumlah	Persentase
Transaksi Normal	18.000	90%
Transaksi Fraud	2.000	10%
Total	20.000	100%

Ketidakseimbangan kelas tersebut menunjukkan bahwa transaksi fraud memiliki proporsi yang jauh lebih kecil dibandingkan transaksi normal. Kondisi ini menjadi salah satu tantangan utama dalam pengembangan sistem deteksi fraud karena model dapat menghasilkan akurasi tinggi hanya dengan memprediksi sebagian besar transaksi sebagai normal. Untuk mengatasi kondisi tersebut, penelitian menerapkan SMOTE pada data pelatihan sehingga model memperoleh representasi kelas fraud yang lebih baik tanpa mengubah data pengujian.

3.1.2 Hasil Feature Engineering

Berdasarkan proses feature engineering, diperoleh beberapa indikator penting yang digunakan dalam proses deteksi fraud dan penilaian risiko.

Tabel 4. Deteksi Fraud dan Penilaian Risiko

Fitur	Fungsi
Transaction Amount	Mengidentifikasi transaksi dengan nilai tidak biasa
Transaction Velocity	Mengidentifikasi lonjakan frekuensi transaksi
Location Deviation	Mengidentifikasi perubahan lokasi yang tidak normal
Device Change	Mengidentifikasi penggunaan perangkat baru
Time Anomaly	Mengidentifikasi transaksi pada waktu tidak biasa
Failed Attempts	Mengidentifikasi aktivitas percobaan transaksi berulang
Historical Risk	Menggunakan riwayat risiko akun
IP Risk	Mengidentifikasi sumber koneksi berisiko

Hasil analisis menunjukkan bahwa Transaction Velocity, Historical Risk, Amount Deviation, Location Deviation, dan Device Change menjadi fitur yang relatif dominan dalam membedakan transaksi normal dan transaksi fraud. Hal ini menunjukkan bahwa karakteristik fraud tidak hanya ditentukan oleh besarnya nominal transaksi. Pola aktivitas dan perubahan perilaku transaksi juga memberikan informasi penting dalam menentukan risiko.

3.1.3 Hasil Perbandingan Model Deteksi Fraud

Empat algoritma digunakan untuk memperoleh model pembanding sebelum diintegrasikan dengan Agentic AI.

Tabel 5. Algoritma model pembanding sebelum diintegrasikan dengan Agentic AI

Model	Accuracy	Precision	Recall	F1-Score	AUC
Logistic Regression	94,1%	82,6%	76,8%	79,6%	0,91
Random Forest	97,2%	91,4%	88,7%	90,0%	0,96
XGBoost	97,8%	92,8%	90,6%	91,7%	0,97

Jurnal Teknologi dan Bisnis
https://journal.stmiki.ac.id
E-ISSN: XXXX-XXXX | P-ISSN: XXXX-XXXX
Vol. 1 No. 1 (2027) | Januari
OPEN ACCESS
https://doi.org/10.63447/jtb.v1i1.2264

Neural Network	97,5%	91,9%	89,8%	90,8%	0,97

Berdasarkan hasil tersebut, XGBoost menghasilkan F1-Score sebesar 91,7% dan AUC sebesar 0,97. Random Forest juga menunjukkan performa yang tinggi dengan F1-Score sebesar 90,0%. Perbedaan antara accuracy dan recall menunjukkan bahwa evaluasi fraud detection tidak cukup dilakukan hanya berdasarkan accuracy. Dalam konteks ini, kemampuan model menemukan transaksi fraud yang sebenarnya ditunjukkan terutama oleh nilai recall.

3.1.4 Pengembangan RiskScore

Untuk mengubah hasil deteksi menjadi tingkat risiko transaksi, penelitian menggunakan formula:

$$\text{RiskScore} = 0{,}35F + 0{,}15A + 0{,}15L + 0{,}20V + 0{,}15H$$

Seluruh komponen dinormalisasi ke rentang 0–100, sehingga RiskScore akhir juga berada pada rentang 0–100. Pembobotan tersebut memberikan kontribusi terbesar kepada probabilitas fraud karena hasil klasifikasi model merupakan indikator utama dalam proses penilaian risiko. Sementara itu, transaction velocity memperoleh bobot kedua terbesar karena perubahan frekuensi transaksi dapat menjadi indikator penting terhadap aktivitas yang tidak normal.
Kategori risiko ditetapkan sebagai berikut:

Tabel 6. Kategori Risiko

RiskScore	Kategori	Tindakan
0–30	Rendah	Approve
31–70	Sedang	Additional Verification
71–100	Tinggi	Flag for Investigation

3.1.5 Distribusi Tingkat Risiko

Setelah mekanisme risk scoring diterapkan terhadap 20.000 transaksi, diperoleh distribusi berikut:

Tabel 7. Distribusi Tingkat Risiko

Tingkat Risiko	Jumlah Transaksi	Persentase
Rendah	16.850	84,25%
Sedang	2.180	10,90%
Tinggi	970	4,85%
Total	20.000	100%

Sebagian besar transaksi berada pada kategori risiko rendah. Sementara itu, sekitar 4,85% transaksi masuk ke kategori risiko tinggi dan memerlukan pemeriksaan lebih lanjut. Menariknya, jumlah transaksi dengan risiko tinggi lebih besar daripada jumlah transaksi fraud aktual. Hal ini menunjukkan bahwa sistem risiko tidak semata-mata melakukan klasifikasi fraud, tetapi juga mengidentifikasi transaksi yang memiliki indikasi perilaku tidak normal meskipun belum tentu merupakan fraud.

3.1.6 Perbandingan Sistem Konvensional dan Agentic AI

Untuk melihat pengaruh integrasi Agentic AI, dilakukan perbandingan antara model klasifikasi biasa dan model yang telah dilengkapi mekanisme risk assessment dan decision agent.

Tabel 8. Perbandingan Model Konvensional dan Agentic AI

Parameter	Model Konvensional	Agentic AI
Accuracy	97,8%	98,3%

Jurnal Teknologi dan Bisnis
https://journal.stmiki.ac.id
E-ISSN: XXXX-XXXX | P-ISSN: XXXX-XXXX
Vol. 1 No. 1 (2027) | Januari
OPEN ACCESS
https://doi.org/10.63447/jtb.v1i1.2264

Precision	92,8%	94,1%
Recall	90,6%	93,2%
F1-Score	91,7%	93,6%
AUC	0,97	0,98
Risk Classification	Tidak tersedia	Tersedia
Decision Recommendation	Tidak tersedia	Tersedia
Contextual Analysis	Terbatas	Terintegrasi

Hasil menunjukkan adanya peningkatan performa setelah model deteksi fraud diintegrasikan dengan mekanisme Agentic AI. F1-Score meningkat dari 91,7% menjadi 93,6%, sedangkan recall meningkat dari 90,6% menjadi 93,2%. Peningkatan tersebut menunjukkan bahwa pendekatan Agentic AI memiliki potensi untuk membantu proses identifikasi transaksi mencurigakan dengan mempertimbangkan lebih banyak konteks transaksi.

3.2 Pembahasan

Hasil penelitian menunjukkan bahwa pendekatan berbasis Agentic AI dapat dikembangkan sebagai mekanisme yang mengintegrasikan fraud detection, risk scoring, dan decision support dalam satu arsitektur. Pendekatan tersebut berbeda dari sistem klasifikasi konvensional yang umumnya berhenti pada keluaran berupa label atau probabilitas fraud. Salah satu temuan penting adalah bahwa probabilitas fraud saja belum cukup untuk menggambarkan keseluruhan risiko transaksi. Dua transaksi dapat memiliki probabilitas fraud yang relatif sama, tetapi memiliki karakteristik risiko yang berbeda apabila dilihat dari lokasi, frekuensi transaksi, perubahan perangkat, maupun riwayat transaksi. Integrasi beberapa indikator melalui formula RiskScore memungkinkan sistem menghasilkan representasi risiko yang lebih terstruktur. Dengan demikian, transaksi tidak hanya dikategorikan sebagai fraud atau normal, tetapi juga dapat ditempatkan pada tingkat risiko rendah, sedang, atau tinggi. Penerapan decision agent juga memberikan nilai tambah dari sisi operasional. Transaksi berisiko rendah dapat diproses secara otomatis, transaksi berisiko sedang dapat diarahkan ke mekanisme verifikasi tambahan, sedangkan transaksi berisiko tinggi dapat ditandai untuk pemeriksaan lebih lanjut. Pola tersebut dapat membantu mengurangi beban pemeriksaan manual terhadap seluruh transaksi.

Namun demikian, hasil penelitian juga menunjukkan bahwa peningkatan kemampuan deteksi perlu diimbangi dengan pengendalian false positive. Jika terlalu banyak transaksi normal dikategorikan berisiko tinggi, sistem dapat mengurangi kenyamanan pengguna dan meningkatkan beban investigasi. Oleh karena itu, pengembangan sistem produksi perlu mempertimbangkan keseimbangan antara kemampuan mendeteksi fraud dan kemampuan mempertahankan transaksi normal. Selain itu, nilai hasil penelitian ini masih bersifat eksperimental berdasarkan dataset yang ada. Oleh sebab itu, performa 98,3% accuracy dan 93,6% F1-Score tidak dapat langsung dianggap sebagai performa sistem pada transaksi pembayaran digital Indonesia. Secara keseluruhan, hasil menunjukkan bahwa integrasi Agentic AI + Fraud Detection + Risk Scoring memberikan kerangka yang lebih komprehensif untuk membangun sistem keamanan pembayaran digital. Kontribusi utama model bukan hanya peningkatan metrik klasifikasi, tetapi juga kemampuan mengubah hasil analitik menjadi tingkat risiko dan rekomendasi tindakan yang dapat digunakan sebagai dasar sistem intelligent transaction monitoring.

4. Kesimpulan

Penelitian ini bertujuan mengembangkan model Agentic Artificial Intelligence (Agentic AI) untuk Deteksi Fraud dan Penilaian Risiko Transaksi pada Ekosistem Pembayaran Digital di Indonesia. Berdasarkan hasil eksperimen menggunakan dataset sebanyak 20.000 transaksi, dapat disimpulkan bahwa integrasi Agentic AI dengan algoritma machine learning berpotensi memberikan pendekatan yang lebih komprehensif dalam mengidentifikasi transaksi mencurigakan dan

E-ISSN: XXXX-XXXX | P-ISSN: XXXX-XXXX
Vol. 1 No. 1 (2027) | Januari
OPEN ACCESS
https://doi.org/10.63447/jtb.v1i1.2264

menentukan tingkat risiko secara adaptif. Hasil pengujian menunjukkan bahwa model Agentic AI memperoleh nilai accuracy sebesar 98,3%, precision 94,1%, recall 93,2%, F1-score 93,6%, dan AUC sebesar 0,98. Dibandingkan dengan model XGBoost sebagai model pembanding, integrasi Agentic AI menunjukkan peningkatan F1-score dari 91,7% menjadi 93,6%. Hasil tersebut mengindikasikan adanya peningkatan kemampuan model dalam mengidentifikasi transaksi fraud berdasarkan skenario eksperimen yang digunakan.

Selain kemampuan klasifikasi, model yang dikembangkan juga mengintegrasikan mekanisme Risk Assessment dan Decision Agent untuk menghasilkan tiga kategori risiko, yaitu rendah, sedang, dan tinggi. Setiap kategori memiliki rekomendasi tindakan yang berbeda, meliputi approve untuk transaksi berisiko rendah, additional verification untuk transaksi berisiko sedang, serta flag for investigation untuk transaksi berisiko tinggi. Mekanisme ini memberikan nilai tambah karena sistem tidak hanya menghasilkan prediksi fraud, tetapi juga menyediakan rekomendasi tindakan berdasarkan hasil analisis berbagai indikator transaksi. Kontribusi utama penelitian ini terletak pada pengembangan kerangka integrasi beberapa agen cerdas yang menjalankan fungsi analisis data, deteksi fraud, penilaian risiko, dan pengambilan keputusan dalam satu mekanisme terstruktur. Pendekatan tersebut berpotensi mendukung pengembangan sistem intelligent fraud monitoring yang lebih adaptif, terutama dalam menghadapi perubahan pola transaksi dan ancaman keamanan pada ekosistem pembayaran digital.

Secara keseluruhan, penelitian ini menunjukkan bahwa Agentic AI memiliki potensi sebagai pendekatan pengembangan sistem deteksi fraud dan penilaian risiko transaksi yang lebih terintegrasi, adaptif, dan berorientasi pada pengambilan keputusan. Implementasi lebih lanjut diharapkan dapat mendukung peningkatan keamanan, kepercayaan, dan keberlanjutan ekosistem pembayaran digital di Indonesia.

5. Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada semua pihak yang telah memberikan dukungan, bantuan, dan kontribusi dalam pelaksanaan penelitian serta penyusunan artikel ini. Apresiasi disampaikan kepada institusi, rekan sejawat, dan pihak-pihak yang telah memberikan masukan serta dukungan selama proses penelitian. Penulis juga menyampaikan terima kasih kepada seluruh pihak yang telah membantu dalam penyediaan data dan proses analisis sehingga penelitian ini dapat diselesaikan dengan baik. Penulis menyadari bahwa penelitian ini masih memiliki keterbatasan. Oleh karena itu, kritik dan saran yang konstruktif sangat diharapkan untuk pengembangan penelitian selanjutnya.

6. Daftar Pustaka

Afifah, E. F. N., Simatangkir, D. W. E., & Faliha, N. S. (2025). Keamanan siber dalam perbankan serta tantangan dan solusi di era digital. Jurnal Multidisiplin Ilmu Akademik, 2(1), 33-42. https://doi.org/10.61722/jmia.v2i1.3119

Anggraini, S., & Fatihaturrizqi, M. (2025). Konvergensi Teknologi Blockchain dan Artificial Intelligence Untuk Meningkatkan Kepercayaan Pelanggan Di Sektor Fintech. Perkivi, 2(1), 1-13. https://doi.org/10.51903/perkivi.v2i1.41

Ardhitha, R., Anugerah, R., & Sutabri, T. (2025). Analisis Penerapan Machine Learning dan Algoritma Anomali untuk Deteksi Penipuan pada Transaksi Digital. Repeater: Publikasi Teknik Informatika dan Jaringan, 3(1), 80-90. https://doi.org/10.62951/repeater.v3i1.345

E-ISSN: XXXX-XXXX | P-ISSN: XXXX-XXXX
Vol. 1 No. 1 (2027) | Januari
OPEN ACCESS
https://doi.org/10.63447/jtb.v1i1.2264

Ilahi, N., & Budiono, I. N. (2024). Penerapan artificial intelligence sebagai inovasi di era disrupsi dalam mengurangi resiko keuangan. Moneta: Jurnal Manajemen & Keuangan Syariah, 3(1), 19-30. https://doi.org/10.35905/moneta.v3i1.10145

Iskandar, R., Rhamadhani, R. F., Utami, A. P., Fitrisam, S. A., & Akbar, M. (2025). Peran Kecerdasan Buatan dalam Meningkatkan Efisiensi dan Transparansi Pasar Keuangan: The Role of Artificial Intelligence in Improving Financial Market Efficiency and Transparency. Economic and Education Journal (Ecoducation), 7(1), 186-207. https://doi.org/10.33503/ecoducation.v7i1.1374

Ismanda, R. S., & Silitonga, M. T. A. (2025). Deteksi hybrid anomali transaksi digital dengan optimasi isolation forest-K-means untuk peningkatan keamanan finansial. Innovative: Journal Of Social Science Research, 5(3), 5749-5765. https://doi.org/10.31004/innovative.v5i3.19791

Mutaqin, J. N., Tonang, A. S. P. A., Herawati, N. A., Yulianty, L. P., & Surendro, K. (2025). Agentic AI untuk Tata Kelola Data Kearsipan Konsisten dan Terstruktur. Jurnal Kearsipan, 20(3), 259-278. https://doi.org/10.46836/jk.visdra4.13

Qur'anisa, Z., Herawati, M., Lisvi, L., Putri, M. H., & Feriyanto, O. (2024). Peran fintech dalam meningkatkan akses keuangan di era digital: Studi literatur. Gemilang: Jurnal Manajemen Dan Akuntansi, 4(3), 99-114. https://doi.org/10.56910/gemilang.v4i3.1573

Ramadani, T., Delopinli, C., Septiawan, R., & Ismanto, E. (2025). Analisis performa algoritma machine learning dalam mendeteksi fraud pada dataset aplikasi kartu kredit. JURNAL FASILKOM, 15(2), 383-390. https://doi.org/10.37859/jf.v15i2.9884

Ramadhan, G. B., Dhenabayu, R., Kautsar, A., Fitro, A., & Ariyani, N. F. (2026). Evaluasi Augmentasi Generatif dan Oversampling pada Berbagai Arsitektur Model untuk Deteksi Penipuan Kartu Kredit: Evaluation of Generative Augmentation and Oversampling Across Model Architectures for Credit Card Fraud Detection. MALCOM: Indonesian Journal of Machine Learning and Computer Science, 6(3), 1402-1414. https://doi.org/10.57152/malcom.v6i3.2821

Riyanto, V., Kom, M., Pangesti, W. E., Kom, M., Nurdin, H., Kom, M., ... & Kom, M. (2026). Artificial Intelligence Terapan untuk Sistem Informasi, Jaringan, dan Aplikasi Digital. PT Bukuloka Literasi Bangsa.

Saputra, I. P. G. D., Kesiman, M. W. A., & Sunarya, I. M. G. (2026). Deteksi Pemalsuan QRIS MPM Statis Menggunakan YOLO, PaddleOCR dan Metode Berbasis Aturan. Bulletin of Computer Science Research, 6(2), 763-775. https://doi.org/10.47065/bulletincsr.v6i2.1020

Sidik, D. P., Darmawan, R. N., & Wibowo, A. P. (2026). Teknologi Cerdas untuk Prediksi Risiko Keuangan: Tinjauan Kritis terhadap Penerapan Machine Learning. RESET: Review of Education, Science, and Technology, 2(1), 65-80. https://doi.org/10.66031/reset.v2i1.676

Tarigan, I. F. (2025). Analisis Pola Tren Transaksi Mencurigakan Pada Aplikasi Dana Sebagai Indikator Fraud Digital Tahun 2020-2024. Jurnal Sistem Informasi, Akuntansi dan Manajemen, 5(2), 259-266. https://doi.org/10.54951/sintama.v5i2.1063

Verawati, Y., Bobihu, S. W. I., Kusumaningati, I. D., Trisnodjojo, B. R., & Thanos, J. G. E. (2026). Analisis Fraud Detection Menggunakan Machine Learning pada Sistem Akuntansi Modern.

E-ISSN: XXXX-XXXX | P-ISSN: XXXX-XXXX
Vol. 1 No. 1 (2027) | Januari
OPEN ACCESS
https://doi.org/10.63447/jtb.v1i1.2264

INVESTASI: Inovasi Jurnal Ekonomi dan Akuntansi, 4(2), 110-120. https://doi.org/10.59696/investasi.v4i2.249

Widjaja, G. (2026). Digitalisasi Sistem Pembayaran Dan Risiko Hukum Ai Dalam Deteksi Fraud: Kepastian Hukum Bagi Pelaku Usaha Dan Konsumen Dalam Ekonomi Finansial Teknologi. Jurnal Ekonomi dan Bisnis, 3(11), 362-375. https://doi.org/10.5281/zenodo.19691383