Volume 4 Number 3, Page 362-375, 2025
Expensive | Jurnal Akuntansi
Online ISSN : 2829-4807 – Print ISSN : 2829-5609

Implementasi Model Pendekatan *Machine Learning* untuk Deteksi *Fraud* pada Transaksi Pembayaran *Digital Paper.Id*

Leoni Safira Syah Husin[1], Elmira Febri Darmayanti[2], Jawoto Nusantoro[3*]

[1,2,3] **Universitas Muhammadiyah Metro, Lampung, Indonesia**

E-mail: leonysafira03@gmail.com [1)]
efdarmayanti@gmail.com [2)]
jawoto46@gmail.com [3*)]

ARTICLE INFO

Article history:
Received 20 Januari 2025
Received in Revised 27 April 2025
Accepted 30 September 2025

Keyword's :
Machine Learning, Fraud Detection, Digital Transactions, Anomaly Analysis.

A B S T R A C T

This study aims to apply a machine learning approach in detecting fraud in digital payment transactions in the Paper.id platform. The study was conducted using the Research and Development (R&D) method with the Cross-Industry Standard Process for Data Mining (CRISP DM) development model, which consists of six main stages, namely business understanding, data understanding, data preparation, modeling, evaluation, and implementation. The analysis process involves data exploration, feature engineering, and the application of anomaly detection techniques and network analysis. The results of the study show that the application of the machine learning approach is significantly able to identify suspicious transaction patterns such as collusion between users, misuse of promotions, and other unusual transactions. The implementation of this system is expected to improve the accuracy of fraud detection, efficiency of transaction data processing, and strengthen data security and user trust in the Paper.id platform.

Penelitian ini bertujuan untuk menerapkan pendekatan *machine learning* dalam mendeteksi *fraud* pada transaksi pembayaran *digital* di *platform Paper.id*. Penelitian dilakukan menggunakan metode *Research and Development* (R&D) dengan model pengembangan *Cross-Industry Standard Process for Data Mining* (CRISP-DM), yang terdiri dari enam tahapan utama yaitu pemahaman bisnis, pemahaman data, persiapan data, pemodelan, evaluasi, dan penerapan. Proses analisis melibatkan eksplorasi data, rekayasa fitur (*feature engineering*), dan penerapan teknik deteksi anomali serta analisis jaringan (*network analysis*). Hasil penelitian menunjukkan bahwa penerapan pendekatan *machine learning* secara signifikan mampu mengidentifikasi pola transaksi mencurigakan seperti kolusi antar pengguna, penyalahgunaan promosi, dan transaksi yang tidak wajar lainnya. Implementasi sistem ini diharapkan dapat meningkatkan akurasi deteksi *fraud*, efisiensi pemrosesan data transaksi, serta memperkuat keamanan data dan kepercayaan pengguna terhadap *platform Paper.id*.

Expensive : Jurnal Akuntansi dan Keuangan
Website : https://scholar.ummetro.ac.id/index.php/expensive

* Corresponding author. *Telp.: +6281-0000-0000; fax: +0-000-000-0000.*
E-mail address: jawoto46@gmail.com
Peer review under responsibility of Expensise: Journal of Accounting and Finance. **2829-4807**.

PENDAHULUAN

Perkembangan teknologi informasi yang pesat dalam beberapa dekade terakhir telah memberikan dampak signifikan terhadap berbagai sektor, salah satunya adalah sektor keuangan digital. Penerapan sistem pembayaran *digital*, seperti *e-commerce, peer-to-peer lending*, dan layanan *fintech* lainnya, semakin meluas. Meskipun teknologi ini menawarkan kemudahan dan efisiensi bagi pengguna, ia juga membuka peluang bagi praktik penipuan yang semakin canggih (Adiwijaya & Maulana, 2023)

Aplikasi transaksi pembayaran *digital*, seperti *Paper.id* telah menjadi *platform* yang semakin berkembang dalam mendukung digitalisasi transaksi keuangan. Namun disisi lain seiring dengan peningkatan jumlah transaksi, risiko penyalahgunaan dan potensi penipuan juga semakin tinggi. Oleh karena itu, diperlukan sistem deteksi yang mampu mengidentifikasi transaksi mencurigakan secara *real-time* guna mencegah tindakan yang dapat merugikan pengguna dan *platform* digital.

Berdasarkan hasil pra *survey* yang telah peneliti lakukan pada beberapa waktu lalu bahwa, *Paper.id* adalah solusi pembayaran dan faktur *digital* terkemuka yang dirancang khusus untuk bisnis di Indonesia. *Platform* ini memungkinkan pengguna membuat faktur tanpa batas dengan mudah, mengotomatiskan pengingat pembayaran, dan mengintegrasikan berbagai metode pembayaran seperti kartu kredit dan kode QR. Sejak diluncurkan, *Paper.id* telah mencapai pertumbuhan yang luar biasa, dengan lebih dari 600.000 pengguna yang memanfaatkan layanannya. Dengan antarmuka yang ramah pengguna dan fitur yang kuat, Paper.id menonjol sebagai alat penting bagi bisnis yang ingin mengoptimalkan operasi keuangan mereka.

Namun, kemajuan ini juga diiringi oleh tantangan yang signifikan, yaitu peningkatan kasus penipuan pada transaksi *digital*. Penipuan pada transaksi digital dapat mengakibatkan kerugian finansial yang besar, merusak reputasi, dan menurunkan kepercayaan konsumen terhadap sistem pembayaran *digital*. Oleh karena itu, deteksi penipuan (*fraud detection*) pada transaksi digital menjadi salah satu tantangan penting yang harus dihadapi oleh para penyedia layanan dan lembaga keuangan.

Menurut Adiwijaya & Maulana (2023) menunjukkan bahwa peningkatan kasus penipuan pada transaksi *digital* sering kali disebabkan oleh kurangnya sistem deteksi yang mampu mengidentifikasi aktivitas mencurigakan secara cepat dan akurat. Hal ini diperkuat oleh temuan Deloitte (2022) yang menyatakan bahwa 70% perusahaan *fintech* di Asia Tenggara, termasuk Indonesia, masih mengandalkan sistem keamanan tradisional yang kurang efektif dalam menghadapi modus penipuan yang semakin kompleks. Oleh karena itu, pengembangan sistem

deteksi penipuan berbasis teknologi mutakhir, seperti *artificial intelligence* (AI), *machine learning* (ML), dan *big data analytics*, menjadi solusi yang semakin mendesak untuk diterapkan.

Berdasarkan data dan penelitian terdahulu, studi oleh (Wibowo et al., 2020) menemukan bahwa sistem deteksi berbasis *machine learning* dapat meningkatkan akurasi dalam mengidentifikasi transaksi mencurigakan, meskipun masih memiliki keterbatasan dalam hal implementasi di platform berskala menengah. Selain itu, penelitian oleh (Sari et al., 2023) membuktikan bahwa penerapan algoritma *anomaly detection* mampu mengurangi potensi *fraud* hingga 30% pada sistem pembayaran digital.

Selain itu, aplikasi *Paper.id* juga rentan terhadap berbagai bentuk serangan *cyber* yang menargetkan transaksi keuangan dapat mengancam keamanan data yang dapat merugikan tidak hanya pengguna individual tetapi juga stabilitas sistem keuangan secara keseluruhan. Dengan pertumbuhan digitalisasi keuangan muncul risiko keamanan yang signifikan, penipuan dalam transaksi *digital* dapat terjadi dalam berbagai bentuk, seperti kolusi antara pembeli dan penjual, manipulasi data transaksi, penggunaan identitas dan akun palsu, *phising*, atau akses illegal terhadap akun pengguna. Hal ini sejalan dengan kondisi di Indonesia, di mana kemudahan akses dan efisiensi transaksi pembayaran *digital* menjadi faktor utama yang mendorong pertumbuhan sektor ini. Berdasarkan laporan Bank Indonesia 2024, volume transaksi pembayaran *digital* di Indonesia mengalami peningkatan sebesar 45% dibandingkan tahun sebelumnya, dengan nilai transaksi yang mencapai lebih dari Rp 500 triliun. Namun, di balik pertumbuhan yang pesat ini, risiko keamanan dan kasus penipuan juga turut meningkat. Hal ini menunjukkan bahwa meskipun transformasi *digital* membawa banyak manfaat, tantangan dalam menjaga keamanan transaksi tetap menjadi prioritas utama.

Peningkatan jumlah transaksi *digital* yang signifikan dalam beberapa tahun terakhir turut berkontribusi pada meningkatnya kasus penipuan yang dimanfaatkan celah dalam sistem pembayaran *digital.*

Table 1. Data Tren Penipuan dalam Transaksi Digital di Indonesia (2020-2024)

Tahun	Jumlah Kasus Penipuan Digital	Kerugian Penipuan (Rp Miliar)	Jenis Penipuan
2020	12.500	800	Transaksi *Online*, dan *Phising*
2021	16.000	1.100	*E-Commerce*, dan Jasa Pengiriman
2022	19.500	1.400	Investasi *Digital*, dan Pembayaran QR
2023	23.000	1.650	Kartu Kredit, dan Pembayaran *Digital*
			Pembayaran *Digital*, dan

2024	28.000	2.000	Data Pribadi

Sumber: *Otoritas Jasa Keuangan (OJK) Dan Kementrian Komunikasi dan Informatika (Kominfo)*

Dari data diatas menunjukkan adanya tren peningkatan pada jumlah kasus penipuan dalam transaksi pembayaran *digital* di Indonesia dari tahun 2020 hingga 2024. Seiring dengan pertumbuhan sektor pembayaran *digital*, jumlah kasus penipuan juga mengalami kenaikan yang signifikan, dimulai dengan 12.500 kasus pada tahun 2020 dan meningkat menjadi 28.000 kasus pada tahun 2024. Begitu pula dengan kerugian finansial yang ditimbulkan, yang mencapai Rp 2.000 miliar pada tahun 2024, meningkat pesat dibandingkan tahun sebelumnya.

Menurut Zhang et al (2020), pengguna teknologi *machine learning* dalam sistem deteksi penipuan telah terbukti meningkatkan akurasi dalam mengidentifikasi pola transaksi yang mencurigakan. Algoritma berbasis kecerdasan buatan dapat menganalisis data transaksi secara *real-time* dan mengenali anomali yang menunjukan indikasi aktivitas penipuan. Dalam menghadapi ancaman penipuan ini, teknologi *machine learning* (ML) dan pendekatan dalam deteksi anomali dan penipuan dalam sistem pembayaran *digital* telah muncul sebagai solusi yang efektif dan efisien. *Machine learning*, khususnya, memiliki kemampuan untuk menganalisis data dalam jumlah besar, mendeteksi anomali dalam data transaksi secara *real-time* dan mengidentifikasi pola-pola transaksi yang tidak biasa atau mencurigakan.

Seiring dengan peningkatan penggunaan algoritma dalam sistem pembayaran *digital*, berbagai pendekatan untuk mengidentifikasi dan mencegah penipuan telah dikembangkan, seperti pada penggunaan pendekatan *machine learning* seperti *Rule-Based Detection*, *Detection Anomaly*, *Network Analysis*, *Cohort Analysis* dan *Feature Engineering*. Pendekatan seperti *Interquartile Range* (IQR) didasarkan pada teori statistik untuk mendeteksi data yang menyimpang jauh dari distribusi normalnya. Menurut Montgometry (2019), teknik statistik seperti IQR digunakan untuk mengidentifikasi pencilan dengan menetapkan ambang batas berdasarkan distribusi data.

Pendekatan ini terbukti lebih efektif daripada metode tradisional yang hanya mengandalkan analisis transaksi individu. Pendekatan ini memungkinkan sistem untuk secara efektif mendeteksi pola transaksi yang tidak wajar, mengurangi risiko kerugian finansial, dan meningkatkan kepercayaan pengguna terhadap layanan transaksi pembayaran digital. Oleh karena itu, penerapan pendekatan *machine learning* dalam deteksi anomali dan penipuan dalam sistem pembayaran *digital* diharapkan dapat memberikan manfaat dan kontribusi yang signifkan, dan menjadikannya langkah proaktif untuk meningkatkan keamanan transaksi *digital* seperti *Paper id*.

Penelitian ini dilatarbelakangi oleh berbagai faktor penting. Pertama, meningkatnya *volume* transaksi *digital* yang signifikan, terutama pada *platform* seperti *Paper.id*, menuntut sistem keamanan yang lebih canggih untuk mengidentifikasi dan mencegah aktivitas penipuan. Kedua, kompleksitas modus penipuan yang terus berkembang, seperti kolusi antara pembeli dan penjual, penyalahgunaan promosi, serta penggunaan akun palsu, memerlukan solusi yang mampu beradaptasi dengan cepat. Ketiga, risiko kerugian finansial dan reputasi yang dihadapi oleh *platform* pembayaran *digital* akibat penipuan mendorong perlunya pendekatan yang lebih proaktif dan efektif dalam mendeteksi anomali transaksi. Penelitian ini bertujuan untuk mengembangkan model pendekatan berbasis *machine learning* yang mampu menganalisis data transaksi secara *real-time* guna mendeteksi aktivitas mencurigakan, seperti transaksi dengan nilai yang tidak wajar, frekuensi transaksi yang terlalu tinggi, atau interaksi antara pembeli dan penjual yang mengindikasikan kolusi. Dengan harapan dapat memberikan kontribusi signifikan untuk menghadapi berbagai risiko *fraud*.

METODE PENELITIAN

Pada penelitian ini metode yang digunakan adalah metode penelitian dan pengembangan R&D (*Research and Development*). Menurut (Sugiyono, 2014), metode R&D adalah penelitian yang digunakan untuk menghasilkan produk tertentu dan menguji keefektifan produk tersebut. Dalam konteks penelitian ini, metode R&D digunakan untuk meningkatkan sistem deteksi *fraud* pada transaksi pembayaran *digital Paper.id* dengan pendekatan *machine learning*.

Dalam rangka penerapan model pendekatan *machine learning* untuk meningkatkan sistem deteksi penipuan terhadap pembayaran *digital Paper.id*, model CRISP-DM (*Cross-Industry Standard Process for Data Mining*) dipilih sebagai pendekatan utama. Dengan menerapkan model CRISP-DM (*Cross-Industry Standard Process for Data Mining*), proyek penerapan pendekatan *machine learning* data dapat dilakukan secara sistematis dengan beberapa tahap, seperti pemahaman bisnis, persiapan data, pemodelan, evaluasi dan penerapan.

Selain itu, model CRISP-DM memberikan ruang bagi pengujian berkelanjutan sepanjang siklus pengembangan. Pengujian ini memastikan bahwa sistem deteksi *fraud* yang diimplementasikan tidak hanya efektif secara teoritis, tetapi juga mampu beradaptasi terhadap perubahan pola serangan atau anomali transaksi yang mungkin terjadi di dunia nyata.

HASIL DAN PEMBAHASAN

Dataset yang digunakan dalam penelitian ini terdiri dari beberapa fitur utama yang digunakan dalam analisis transaksi. Data ini diperoleh dari perusahaan *Paper.id* yang mencerminkan aktivitas pengguna terkait pembayaran *digital*. Setiap dataset memiliki karakteristik spesifik yang dapat digunakan untuk mengidentifikasi pola transaksi normal maupun yang berpotensi *fraud*.

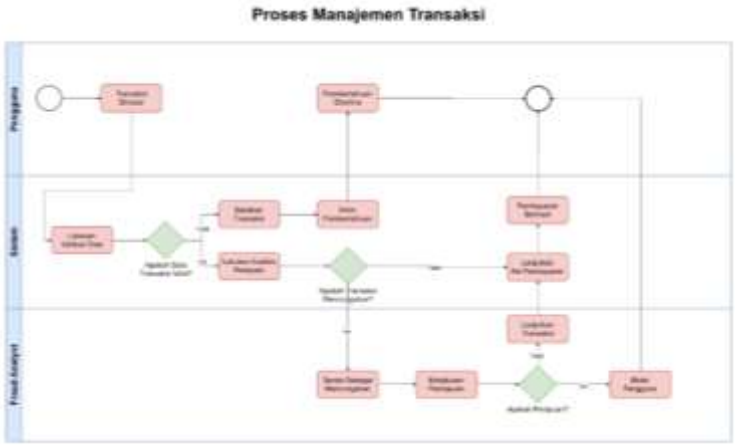
Tabel 2. Deskripsi Dataset Uji Coba

No	Nama Dataset	Jumlah Data	Deskripsi
1	dim_paper_user	50.000	Data pengguna, termasuk informasi akun dan verifikasi.
2	dim_paper_promotion	50.000	Data promosi yang diterapkan pada transaksi.
3	fact_paper_digital_payment_ request	50.000	Data permintaan pembayaran digital.
4	fact_paper_digital_payment_ transaction	50.000	Data transaksi pembayaran digital.

Setiap dataset menyimpan informasi yang berbeda, namun saling melengkapi dalam mendeteksi potensi *fraud* dalam transaksi digital. Kombinasi data pengguna, promosi, serta aktivitas transaksi memungkinkan penerapan pendekatan *machine learning* untuk mengenali pola-pola yang mencurigakan. Dengan analisis lebih lanjut, dataset ini dapat digunakan untuk meningkatkan deteksi keamanan sistem dan mengurangi risiko penipuan di *platform Paper.id*.

Pemodelan Bisnis dan Analisis Aliran Penipuan

Proses deteksi dan penanganan penipuan pada *platform Paper.id* telah dimodelkan menggunakan *Business Process Model and Notation* (BPMN). Proses ini mencakup langkah-langkah utama yang menggambarkan interaksi antara pengguna, sistem, dan bagian penanganan penipuan. Berikut adalah alur lengkap proses BPMN:



Gambar 1. Diagram Business Process Model and Notation

Dari diagram diatas, terdapat 5 tahapan dalam melakukan analisis penipuan pada transaksi yang dilakukan oleh pengguna pada *platform Paper.id*. berikut adalah 5 tahapan tersebut meliputi:

a. Inisialisasi Transaksi

   Proses diawali ketika pengguna melakukan sebuah transaksi atau mengajukan sebuah transaksi pada *Paper.id*. Pada tahap ini, sistem akan secara otomatis melakukan validasi data dari transaksi yang diajukan oleh pengguna, seperti informasi pembeli, penjual, jumlah transaksi, metode pembayaraan, dan waktu transaksi.

b. Validasi Data

   Sistem secara otomatis melakukan verifikasi informasi transaksii, termasuk jumlah pembayaran, metode yang digunakan, serta status akan pengguna.

c. Pendeteksian Anomali Awal

   Sistem menerapkan algoritma pendeteksian berbasis berbasis aturan (*rule-based*) dan pembelajaran mesin (*machine learning*) untuk mengidentifikasi potensi *fraud* sebelum transaksi diproses lebih lanjut.

d. Konfirmasi dan Proses Pembayaran

   Jika transaksi lolos validasi dan tidak terindikasi sebagai *fraud*, sistem akan meneruskan transaksi ke tahap pembayaran.

e. Pemantauan dan Evaluasi

   Setelah transaksi berhasil diproses, sistem terus memantau pola transaksi pengguna untuk meningkatkan model deteksi *fraud* berdasarkan data terbaru.

Data Cleaning

Agar hasil analisis lebih akurat, data transaksi perlu melalui proses data *cleaning* untuk menghilangkan anomali, data tidak *valid*, atau inkonsisten yang dapat mempengaruhi kinerja model. Berikut adalah tahapan utama dalam proses pembersihan data:

a. Identifikasi dan Penghapusan Data Duplikat

   Dataset menunjukkan adanya 40.473 data duplikat dalam dataset promosi, lalu data duplikat dihapus untuk mencegah redundansi dalam model dan memastikan analisis yang lebih akurat.

b. Penanganan *Missing Value*

   Beberapa atribut, seperti kode promosi dan status akun pengguna, ditemukan memiliki nilai kosong. Nilai yang kosong diisi dengan metode imputasi berdasarkan modus, sementara atribut kategori seperti kode promosi diberikan label khusus (‘*No Promotion’*) agar tidak mempengaruhi pola transaksi yang dianalisis.

c. Normalisasi Data

Untuk memastikan bahwa model *machine learning* dapat bekerja dengan baik, atribut numerik seperti *transaction_amount* dan *total_fee_amount* dinormalisasikan menggunakan *Min-Max Scaling*. Normalisasi ini bertujuan untuk menyamakan skala data sehingga distribusi nilai transaksi lebih seragam, menghindari dominasi fitur tertentu dalam proses prediksi.

Feature Engineering

Rekayasa fitur ini dilakukan untuk menciptakan fitur-fitur yang dapat membantu model *machine learning* dalam mendeteksi transaksi mencurigakan. Beberapa fitur utama yang dikembangkan dalam penelitian ini meliputi:

a. *Buyer-Seller Relationship Score*

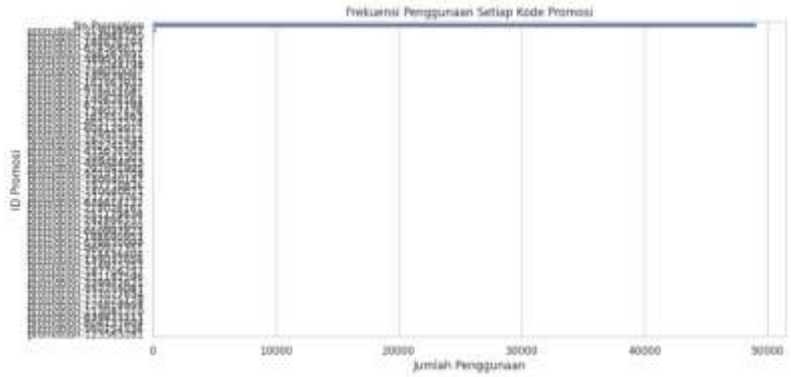
Menghitung hubungan antara pembeli dan penjual berdasarkan jumlah transaksi yang dilakukan antara dua akun yang sama dalam kurun waktu tertentu. Jika jumlah transaksi yang terjadi antara dua akun tertentu melebihi 3 kali lipat dari rata-rata, hubungan ini dianggap tidak wajar dan menjadi indikasi *fraud*.

b. *Time Gap Analysis*

Mengukur selisih waktu antar transaksi untuk mendeteksi lonjakan aktivitas yang tidak biasa. Jika suatu akun melakukan transaksi dalam interval kurang dari 5 menit secara berulang, transaksi tersebut dikategorikan sebagai mencurigakan.

c. Penyalahgunaan Promosi

Mengidentifikasi pengguna yang menggunakan kode promosi lebih dari 10 kali dalam periode 24 jam, yang dapat menjadi indikasi eksploitasi sistem promosi *Paper.id*.



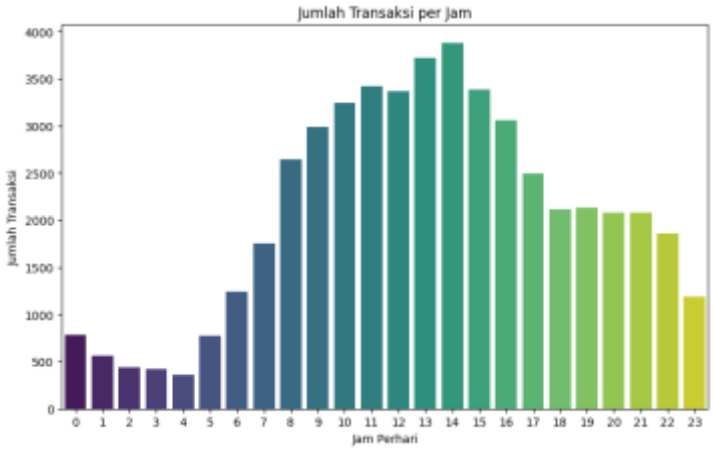
Gambar 2. Visualisasi Penyalahgunaan Promosi

Dari grafik batang di atas, dapat disimpulkan bahwa transaksi yang dilakukan cenderung minim menggunakan kode promosi.

Analisis Pola Transaksi

a. Analisis Transaksi Berdasarkan Waktu Operasional

Berdasakan hasil analisis, ditemukan bahwa puncak transaksi terjadi pada pukul 14.00, yang kemungkinan besar terkait dengan waktu istirahat siang pengguna. Aktivitas transaksi tetap tinggi hingga malam hari, terutama menjelang tengah malam, yang meningkatkan kemungkinan terjadinya penipuan. Seperti yang terlihat pada hasil visualisasi berikut:

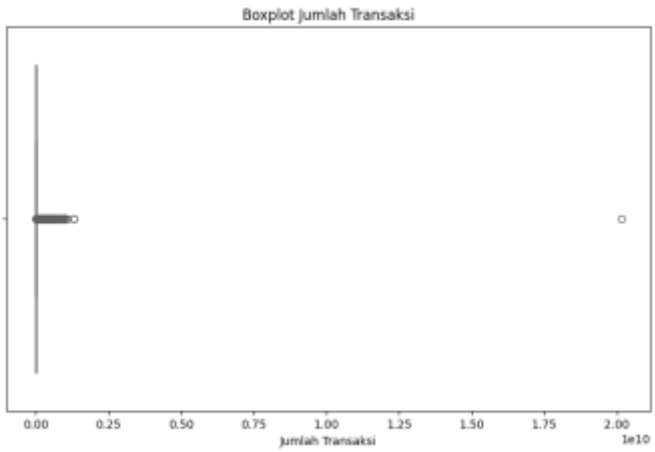


Gambar 3. Visualisasi Jumlah Transaksi Berdasarkan Waktu

Berdasarkan grafik di atas, dapat disimpulkan bahwa pihak *Paper.id* perlu berhati-hati selama periode puncak transaksi, karena meningkatnya jumlah transaksi sering kali diiringi dengan potensi kasus penipuan yang lebih tinggi.

b. Analisis Anomali dalam Nilai Transaksi

Tahapan ini bertujuan untuk menganalisis distribusi dan karakteristik nilai transaksi (*transaction_amount*) dalam dataset. Berikut terdapat diagram yang menggambarkan distribusi serta karakteristik dari jumlah transaksi yang ada dengan menggunakan metode IQR.



Gambar 4. Visualisasi Anomali dalam Transaksi

Berdasarkan grafik *Boxplot* ini, dapat disimpulkan bahwa sebagian besar transaksi yang terjadi memiliki nilai yang sangat kecil. Hanya ada sedikit sekali transaksi dengan nilai yang besar, dan transaksi-transaksi inilah yang menjadi *outlier*. Distribusi data juga tidak simetris, dengan sebagian besar data terkonsentrasi di bagian bawah.

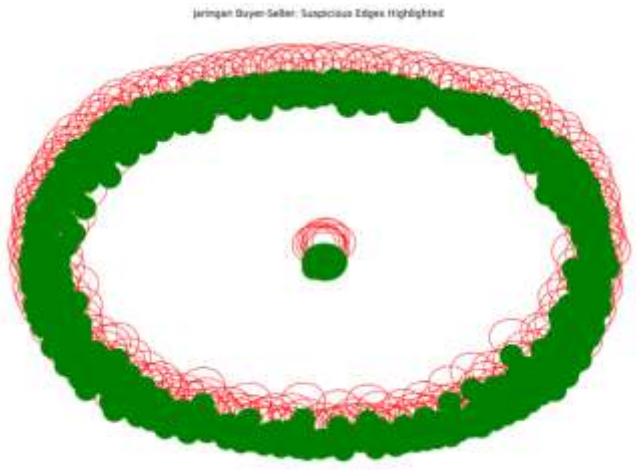
c. Analisis Hubungan Pembeli dan Penjual Mencurigakan

Beberapa akun memiliki jumlah transaksi tinggi dalam pola berulang antara pembeli dan penjual yang sama, yang dapat menjadi indikasi skema pencucian uang atau penipuan.

Table 3. Data Pasangan Pembeli dan Penjual Mencurigakan

No	buyer_id	seller_id	Jumlah Transaksi	Total Transaksi (IDR)
1	0bb440f2….	0bb440f2….	1,266	104.356.543
2	10f3200a….	10f3200a….	321	14.801.810
3	34d1c64b….	34d1c64b….	294	17.074.390

Data pada tabel di atas diambil dari hasil menjalankan *query*, dengan tiga data teratas yang dipilih. Dari hasil tersebut, terlihat bahwa terdapat beberapa pengguna (*buyer_id* dan *seller_id*) yang memiliki jumlah transaksi yang sangat tinggi dibandingkan dengan yang lainnya. Sebagai contoh, transaksi dengan jumlah *transaction_amount* yang jauh lebih tinggi dari rata-rata menunjukkan adanya perilaku transaksi yang mencurigakan atau tidak wajar, yang perlu dicermati lebih lanjut. Hasil dari pasangan pengguna yang sudah terlihat akan dianalisis lebih lanjut dengan visualisasi jaringan antara pembeli dan penjual menggunakan alat seperti *NetworkX* pada *Python* dimana untuk menunjukkan hubungan dan menyoroti interaksi yang mencurigakan. Adapun hasil outputnya yaitu sebagai berikut:



Gambar 5. Visualisasi Jaringan Pengguna

Berdasarkan visualisasi ini beberapa interpretasi yang dapat disimpulkan bahwa, node-node pusat yang memiliki banyak koneksi keluar (edge) berwarna merah kemungkinan besar

terlibat dalam banyak transaksi yang mencurigakan. Ini karena edge berwarna merah mengindikasikan bobot yang tinggi, yang dalam konteks ini mungkin mewakili jumlah transaksi atau nilai transaksi yang besar. Komunitas-komunitas yang memiliki banyak edge berwarna merah mungkin merupakan kelompok penipu yang bekerja sama.

Evaluasi Model Machine Learning

Model pendekatan Machine Learning yang digunakan dalam penelitian ini dievaluasi menggunakan beberapa metrik utama untuk menilai performa deteksi *fraud*. Metrik ini digunakan untuk mengukur seberapa baik model dapat membedakan transaksi yang sah dan yang berpotensi *fraud*.

Table 4. Data Evaluasi Model Machine Learning

No	Metrik	Nilai (%)
1	Akurasi	85%
2	Precision	80%
3	Recall	90%
4	F1-Score	85%

Berdasarkan hasil evaluasi, model *Machine Learning* yang diterapkan memiliki kinerja yang cukup baik dalam deteksi *fraud*. Hal ini ditunjukkan oleh nilai akurasi sebesar 85%, yang mengindikasikan bahwa sebagian besar prediksi yang dihasilkan model sudah sesuai dengan kondisi sebenarnya. Selain itu, 80% menunjukkan bahwa dari semua transaksi yang diklasifikasikan sebagai fraud, 80% di antaranya memang benar-benar *fraud*, sehingga model mampu mengurangi jumlah *false positive*. *Recall* yang mencapai 90% menandakan bahwa model mampu mengidentifikasi sebagian besar transaksi *fraud* yang ada dalam dataset, meskipun masih ada beberapa yang terlewat. Sementara itu, nilai *F1-Score* sebesar 85% menunjukkan keseimbangan antara *precision* dan *recall*, yang mengindikasikan bahwa model memiliki performa yang stabil dan dapat diandalkan untuk deteksi *fraud* dalam transaksi pembayaran *digital*.

KESIMPULAN DAN SARAN

Penelitian ini bertujuan untuk menerapkan pendekatan Machine Learning dalam mendeteksi transaksi fraud pada sistem pembayaran digital Paper.id. Model yang dikembangkan dirancang untuk mengenali pola-pola transaksi mencurigakan berdasarkan data historis yang tersedia. Berdasarkan hasil analisis dan pengujian, model deteksi fraud menunjukkan kinerja yang cukup baik dalam mengklasifikasikan transaksi berisiko penipuan. Dengan memanfaatkan teknik pembelajaran mesin, model ini mampu mengenali karakteristik utama dari aktivitas yang mencurigakan sehingga dapat mendukung proses mitigasi risiko secara lebih cepat dan efisien.

Namun demikian, evaluasi hasil pengujian mengindikasikan bahwa masih terdapat beberapa aspek yang perlu ditingkatkan. Salah satu tantangan utama adalah tingginya tingkat *false positive*, di mana transaksi sah diklasifikasikan sebagai fraud. Selain itu, keterbatasan dataset dalam hal ukuran dan keragaman juga menjadi hambatan dalam meningkatkan generalisasi model terhadap pola transaksi yang berbeda.

Dengan menerapkan saran-saran pengembangan Sistem Keamanan yang Lebih Adaptif ini, diharapkan model deteksi *fraud* yang telah dikembangkan dapat semakin optimal dalam mengidentifikasi transaksi mencurigakan serta memberikan kontribusi yang lebih besar dalam meningkatkan kemanan sistem pembayaran *digital Paper.id*.

DAFTAR PUSTAKA

Adiwijaya, A. P., & Maulana, W. S. (2023). Analisis Pembuatan Sistem Antifraud Pada Startup Fintech, Khususnya Peer-To-Peer Lending. *Jurnal Ilmiah Teknik*, *2*(3), 69–76. https://doi.org/10.56127/juit.v2i3.1188

Albrecht, C. C., Albercht, W. S., & Dunn, J. G. (2019). *Fraud Examination. 6th ed*. Cengage Learning.

Ardhitha, R., Anugerah, R., & Sutabri, T. (2025). *Analisis Penerapan Machine Learning dan Algoritma Anomali untuk Deteksi Penipuan pada Transaksi Digital*. *1*, 80–90.

Barabási. (2016). *Network Science*. Cambridge University Press.

Brownlee, J. (2016). *Feature Selection For Machine Learning in Python*. https://machinelearningmastery.com/feature-selection-machine-learning-python/

Cressey, D. R. (1953). *Other People's Money*. Patterson Smith.

Deloitte. (2022). Southeast Asia Fintech Report: Challenges and Opportunities in Fraud Preverention. *Delloitte Insights*.

Domingos, P. (2012). A Few Useful Things to Know about Machine Learning. *Communications of the ACM*, *55*(10), 78–87. https://doi.org/10.1145/2347736.2347755

Eldo, H., Ayuliana, A., Suryadi, D., Chrisnawati, G., & Judijanto, L. (2024). Penggunaan Algoritma Support Vector Machine (SVM) Untuk Deteksi Penipuan pada Transaksi Online. *Jurnal Minfo Polgan*, *13*(2), 1627–1632. https://doi.org/10.33395/jmp.v13i2.14186

Febriyani, W., Supratman, N. A., & Witjaksono, R. W. (2024). *Exploring the Contribution of Fintech to Digital Transformation in Indonesian MSMEs : A Literature Review*. *13*(6), 2564–2572. https://doi.org/10.32520/stmsi.v13i6.4638

Gee, J. (2014). *The Financial Fraud Handbook: Fraud Preverention and Detection Strategies*. Wiley.

Guyon, I., & Elisseeff, A. (2003). An Introduction to Variable and Feature Selection 1 Introduction. *Journal of Machine Learning Research (JMLR)*, *3*, 1157–1182.

Japit, S., Risyani, Y., Selamat, T., Bombongan, C., & Yuliana, Y. (2024). Deteksi Anomali Transaksi E-Commerce Menggunakan Support Vector Machine Berbasis Data Mining. *Jurnal Minfo Polgan*, *13*(2), 1976–1980.

McKinsey, G. I. (2016). *Digital Finance for All : Powering Inclusive Growth in Emerging Economies* (Issue September). McKinsey & Company.

Montgometry, D. C. (2019). *Introduction to Statistical Quality Control* (8th ed.). Wiley.

Newman, M. E. J. (2003). The structure and function of complex networks. In *SIAM Review* (Vol. 45, Issue 2). Society for Industrial and Applied Mathematics (SIAM).

Nurhayati, Busman, & Iswara, R. P. (2019). PENGEMBANGAN ALGORITMA UNSUPERVIS

ED LEARNING TECHNIQUE PADA BIG DATA ANALYSIS DI MEDIA SOSIAL SEBAGAI MEDIA PROMOSI. *Jurnal Teknik Informatika*, *12*(1), 79–96. https://doi.org/10.15408/jti.v12i1.11342

Otoritas Jasa Keuangan (OJK) Dan Kementrian Komunikasi dan Informatika (Kominfo). (2024). *Data Tren Penipuan dalam Transaksi Digital di Indonesia*. Di Akses Pada Januari 2025.

Pamungkas, F. S., Prasetya, B. D., & Kharisudin, I. (2020). Perbandingan Metode Klasifikasi Supervised Learning pada Data Bank Customers Menggunakan Python. *PRISMA, Prosiding Seminar Nasional Matematika*, *3*, 692–697. https://journal.unnes.ac.id/sju/index.php/prisma/article/view/37875

Qiang, W., & Zhongli, Z. (2011). Reinforcement learning model, algorithms and its application. *Proceedings 2011 International Conference on Mechatronic Science, Electric Engineering and Computer, MEC 2011*, 1143–1146. https://doi.org/10.1109/MEC.2011.6025669

Rahardjo, A., Setiawan, D., & Lestari, P. (2021). ingkat Kesadaran Pengguna terhadap Keamanan Transaksi Digital di Indonesia: Sistem Deteksi Penipuan pada Beberapa Platform. *Jurnal Riset Keuangan Dan Akuntansi*, *7*(2), 134–142.

Rauhan, A. (2019). Pengolahan Data Menggunakan Machine Learning. *Student Paper Pertamina University*, *021*, 1–4. https://library.universitaspertamina.ac.id/xmlui/bitstream/handle/123456789/162/Jur

Retnoningsih, E., & Pramudita, R. (2020). Mengenal Machine Learning Dengan Teknik Supervised Dan Unsupervised Learning Menggunakan Python. *Bina Insani Ict Journal*, *7*(2), 156. https://doi.org/10.51211/biict.v7i2.1422

Sallu, S.-, & Qammaddin, Q. (2020). Keamanan Data Pembelajaran Online Jaringan Komputer di Perguruan Tinggi. *Instruksional*, *2*(1), 239–244. https://doi.org/10.24853/Instruksional.2.1.35-40

Santoso, P., Abijono, A., & Anggreini, N. L. (2021). Algoritma Supervised Learning Dan Unsupervised Learning Dalam Pengolahan Data. *Jurnal Teknologi Terapan: G-Tech*, *4*(2), 315–318. https://doi.org/10.33379/gtech.v4i2.635

Simeone, O. (2018). A Brief Introduction to Machine Learning for Engineers. In *Foundations and Trends in Signal Processing* (Vol. 12, Issues 3–4). https://doi.org/10.1561/2000000102

Sugiyono. (2014). *Metode penelitian bisnis: pendekatan kuantitatif, kualitatif, kombinasi, dan R&D*. Alfabeta.

Wang, C., Dou, Y., Chen, M., Chen, J., Liu, Z., & Yu, P. S. (2021). Fraud Detection Using Network Analysis and Machine Learning Techniques. *Journal of Financial Technology*, *1*, 1–4. https://arxiv.org/abs/2110.01171

Watson, H. J., Grecich, D. G., Shearer, C., Hammer, K., Herdlein, S. a, Moncla, B., Davidovic, G., Fong, J., Wong, H. K., & Fong, A. (2000). The CRISP-DM Model: The New Blueprint for

Data Mining. *Journal of Data Warehousing*, *5*(4), 15–18.

Wibowo, A., Darwati, I., & Irnawati, O. (2020). Prediksi Operasi Sesar Dengan Machine Learning. *J I M P - Jurnal Informatika Merdeka Pasuruan*, *4*(3). https://doi.org/10.37438/jimp.v4i3.228

Yosephine, V. S., Hanna, T., Setiawati, M., & Setiawan, A. (2023). Machine Learning for Quality Control in Traditional Textile Manufacturing. *Jurnal Rekayasa Sistem Industri*, *13*(1), 165–174. https://doi.org/10.26593/jrsi.v13i1.7173.165-174

Zhang, Z., Chen, L., Liu, Q., & Wang, P. (2020). A Fraud Detection Method for Low-Frequency Transaction. *IEEE Access*, *8*, 25210–25220. https://doi.org/10.1109/ACCESS.2020.2970614

Zheng, A., & Casari, A. (2018). *Feature Engineering for Machine Learning: Principles and Techniques for Data Scientist*. O'Reilly Media.