Repeater : Publikasi Teknik Informatika dan Jaringan
Volume. 3, No. 1, Januari 2025
e-ISSN : 3046-7276; dan p-ISSN : 3046-7284; Hal. 80-90
DOI: https://doi.org/10.62951/repeater.v3i1.345
Available online at: https://journal.aptii.or.id/index.php/Repeater

Analisis Penerapan Machine Learning dan Algoritma Anomali untuk Deteksi Penipuan pada Transaksi Digital

Reyhand Ardhitha[1] , Revifal Anugerah[2] , Tata Sutabri[3]
[1-3] Universitas Bina Darma Palembang, Indonesia
[1]reyhandardhitha@gmail.com, [2]revifalanugerah1@gmail.com, [3]tata.sutabri@gmail.com

Abstract. *Fraud in digital transactions has become a serious issue threatening the security and integrity of the fintech and e-commerce sectors. To address this problem, machine learning technology has emerged as an effective solution for automatically detecting anomalies and fraudulent transactions. This study aims to analyze the application of machine learning algorithms, specifically Support Vector Machine (SVM), Random Forest, and Ensemble Learning, in detecting fraud in digital transactions. The research adopts a quantitative approach with experimentation, testing the effectiveness of the three algorithms using a digital transaction dataset consisting of both fraudulent and non-fraudulent transactions. The results show that the Random Forest algorithm performs the best in terms of accuracy and recall, followed by Ensemble Learning, which enhances fraud detection performance by combining multiple prediction models. Meanwhile, SVM demonstrates satisfactory performance but is prone to overfitting issues when handling large and complex datasets. The study also finds that the problem of imbalanced data can affect model accuracy, and data balancing techniques such as oversampling are required to improve fraud detection performance. Overall, the findings suggest that machine learning, particularly Random Forest and Ensemble Learning algorithms, can be relied upon to improve fraud detection in digital transactions. However, challenges such as model interpretability and the need for periodic algorithm updates still need to be addressed to enhance the effectiveness of fraud prevention systems in countering the ever-evolving nature of fraud.*

Keywords*: Machine Learning, Fraud Detection, Digital Transactions.*

Abstrak. Penipuan dalam transaksi digital telah menjadi masalah serius yang mengancam keamanan dan integritas sektor fintech dan e-commerce. Untuk mengatasi masalah ini, teknologi machine learning telah berkembang sebagai solusi yang efektif untuk mendeteksi anomali dan transaksi fraud secara otomatis. Penelitian ini bertujuan untuk menganalisis penerapan algoritma machine learning, khususnya Support Vector Machine (SVM), Random Forest, dan Ensemble Learning, dalam mendeteksi penipuan pada transaksi digital. Penelitian ini menggunakan pendekatan kuantitatif dengan eksperimen, menguji efektivitas ketiga algoritma menggunakan dataset transaksi digital yang mencakup transaksi fraud dan non-fraud. Hasil penelitian menunjukkan bahwa algoritma Random Forest memberikan kinerja terbaik dalam hal akurasi dan recall, diikuti oleh Ensemble Learning, yang mampu meningkatkan kinerja deteksi penipuan dengan menggabungkan beberapa model prediksi. Sementara itu, SVM menunjukkan kinerja yang cukup baik meskipun rentan terhadap masalah overfitting ketika dataset besar dan kompleks. Penelitian ini juga menemukan bahwa masalah ketidakseimbangan data (imbalanced data) dapat memengaruhi akurasi model, dan teknik penyeimbangan data seperti oversampling diperlukan untuk meningkatkan performa deteksi penipuan. Secara keseluruhan, hasil penelitian ini menunjukkan bahwa machine learning, khususnya algoritma Random Forest dan Ensemble Learning, dapat diandalkan untuk meningkatkan deteksi penipuan pada transaksi digital, meskipun beberapa tantangan seperti interpretabilitas model dan kebutuhan pembaruan algoritma secara berkala masih perlu diatasi untuk meningkatkan keefektifan sistem antifraud dalam menghadapi penipuan yang terus berkembang.

Kata kunci: Machine Learning, Deteksi Penipuan, Transaksi Digital.

1. 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

Received: Desember 06, 2024; Revised: Desember 21, 2024; Accepted: Januari 04 , 2025;
Published: Januari 07, 2025;

semakin canggih (Adiwijaya & Maulana, 2023). 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.

Dalam menghadapi ancaman penipuan ini, teknologi machine learning (ML) dan algoritma deteksi anomali telah muncul sebagai solusi yang efektif dan efisien. Machine learning, khususnya, memiliki kemampuan untuk menganalisis data dalam jumlah besar dan mengidentifikasi pola-pola transaksi yang tidak biasa atau mencurigakan. Hal ini memungkinkan sistem untuk mendeteksi penipuan secara lebih akurat dan lebih cepat daripada metode konvensional yang sering bergantung pada aturan yang telah ditetapkan sebelumnya (Eldo et al., 2024). Algoritma deteksi anomali dalam konteks ini dapat digunakan untuk memeriksa ketidakwajaran dalam pola transaksi yang mungkin menunjukkan adanya penipuan (Japit et al., 2024).

Seiring dengan peningkatan penggunaan algoritma berbasis kecerdasan buatan (AI) dalam sistem pembayaran digital, berbagai pendekatan untuk mengidentifikasi dan mencegah penipuan telah dikembangkan. Salah satunya adalah penggunaan algoritma seperti Support Vector Machine (SVM), Random Forest, dan Ensemble Learning. Algoritma-algoritma ini memiliki keunggulan dalam menangani data yang tidak seimbang dan dapat mengenali anomali dalam transaksi yang tidak terdeteksi oleh sistem tradisional (Kolbia & Dahliyanti, 2024; Saputra et al., 2024). Misalnya, SVM digunakan untuk mengklasifikasikan transaksi sebagai fraud atau non-fraud berdasarkan fitur-fitur tertentu yang diambil dari data transaksi sebelumnya (Eldo et al., 2024). Di sisi lain, algoritma Random Forest dan Ensemble Learning menggabungkan banyak model prediksi untuk meningkatkan akurasi deteksi penipuan (Lubis & Andri, 2024).

Selain itu, penerapan teknologi blockchain dalam sektor fintech juga semakin mendapat perhatian, terutama dalam meningkatkan keamanan dan transparansi transaksi. Teknologi ini memungkinkan pencatatan transaksi yang bersifat permanen dan tidak dapat diubah, yang dapat mengurangi risiko terjadinya penipuan (Caseba & Dewayanto, 2024). Dengan mengintegrasikan blockchain dengan sistem deteksi penipuan berbasis machine learning, diharapkan dapat tercipta ekosistem digital yang lebih aman dan terjamin dari risiko penipuan.

Namun, meskipun teknologi ini menjanjikan, tantangan tetap ada dalam penerapannya. Salah satu tantangan utama adalah kompleksitas data yang terus berkembang

dan kemungkinan terjadinya perubahan pola penipuan yang tidak terduga. Penipuan digital yang dilakukan oleh para pelaku kejahatan semakin canggih dengan menggunakan berbagai teknik, seperti pengelabuan identitas dan manipulasi data. Oleh karena itu, sistem deteksi penipuan harus dapat beradaptasi dengan cepat terhadap perubahan pola penipuan dan dapat mengidentifikasi potensi ancaman yang sebelumnya tidak terdeteksi (Judijanto et al., 2024). Penelitian terkait penerapan machine learning dalam deteksi penipuan masih terus berkembang, dengan berbagai algoritma yang diuji untuk meningkatkan efektivitas dan efisiensi deteksi fraud.

Pentingnya penelitian ini terletak pada kemampuan teknologi machine learning dan algoritma deteksi anomali dalam memberikan solusi inovatif terhadap masalah penipuan transaksi digital. Penelitian ini bertujuan untuk mengkaji penerapan algoritma machine learning dan deteksi anomali dalam mendeteksi penipuan pada transaksi digital dengan mempertimbangkan berbagai aspek, seperti akurasi, kecepatan, dan kemampuan untuk beradaptasi dengan pola penipuan yang baru. Melalui kajian ini, diharapkan dapat diperoleh pemahaman yang lebih baik mengenai efektivitas berbagai algoritma dalam mendeteksi penipuan serta tantangan yang dihadapi dalam implementasinya.

Dalam pengembangan sistem antifraud berbasis machine learning, banyak perusahaan fintech yang telah mulai menerapkan pendekatan ini untuk meningkatkan keamanan dan kenyamanan penggunanya. Sebagai contoh, pada platform peer-to-peer lending, penerapan algoritma machine learning memungkinkan analisis risiko kredit secara lebih akurat dan meminimalkan potensi terjadinya penipuan dalam pengajuan pinjaman (Adiwijaya & Maulana, 2023). Demikian juga dalam e-commerce, algoritma deteksi anomali dapat digunakan untuk memantau transaksi secara real-time dan mendeteksi transaksi yang mencurigakan, yang berpotensi merugikan baik penjual maupun pembeli (Valentino, 2023).

Meskipun demikian, penerapan teknologi ini tidak lepas dari berbagai kendala dan tantangan. Salah satunya adalah permasalahan terkait privasi dan keamanan data pengguna. Penggunaan data transaksi yang sangat besar dan beragam memerlukan pendekatan yang hati-hati dalam hal pengelolaan dan perlindungan data pribadi. Oleh karena itu, penting untuk memastikan bahwa implementasi sistem deteksi penipuan berbasis machine learning tidak hanya efektif dalam mendeteksi fraud, tetapi juga menjaga agar data pengguna tetap aman dan terlindungi dari ancaman penyalahgunaan.

Secara keseluruhan, perkembangan teknologi machine learning dan algoritma deteksi anomali membuka peluang besar dalam mencegah dan mendeteksi penipuan pada transaksi digital. Penerapan teknologi ini dapat membantu mengurangi kerugian yang ditimbulkan akibat

penipuan dan meningkatkan kepercayaan konsumen terhadap sistem pembayaran digital. Namun, untuk dapat memaksimalkan potensi teknologi ini, diperlukan riset lebih lanjut dan kolaborasi antara pengembang teknologi, regulator, dan penyedia layanan keuangan untuk mengatasi tantangan yang ada dan memastikan keamanan transaksi digital di masa depan.

2. METODE

Metode penelitian yang digunakan dalam studi ini adalah pendekatan kuantitatif dengan menggabungkan studi literatur dan eksperimen untuk mengevaluasi penerapan machine learning dan algoritma deteksi anomali dalam mendeteksi penipuan pada transaksi digital. Pendekatan ini dipilih karena penelitian ini bertujuan untuk menganalisis efektivitas berbagai algoritma dalam menangani kasus penipuan yang terjadi pada transaksi digital dan mengeksplorasi potensi penerapan algoritma machine learning dalam sistem antifraud di sektor fintech dan e-commerce.

Tahap pertama dalam penelitian ini adalah studi literatur yang bertujuan untuk mengumpulkan informasi terkait dengan penerapan machine learning dalam deteksi penipuan pada transaksi digital. Penelusuran literatur dilakukan dengan merujuk pada berbagai jurnal, artikel ilmiah, dan buku yang membahas topik algoritma machine learning, algoritma deteksi anomali, serta penerapannya dalam mendeteksi penipuan pada sektor fintech dan e-commerce. Beberapa algoritma yang dipelajari dalam studi literatur ini meliputi Support Vector Machine (SVM), Random Forest, dan Ensemble Learning, yang dikenal memiliki kemampuan untuk mengatasi dataset yang tidak seimbang serta mendeteksi pola transaksi yang mencurigakan dan tidak biasa (Eldo et al., 2024; Saputra et al., 2024). Studi literatur ini juga bertujuan untuk memahami tantangan yang dihadapi dalam implementasi algoritma-algoritma tersebut serta kontribusinya terhadap sistem deteksi penipuan.

Setelah melakukan studi literatur, tahap berikutnya adalah pengumpulan data yang akan digunakan untuk menguji dan mengevaluasi efektivitas algoritma machine learning dalam mendeteksi penipuan. Dataset yang digunakan dalam penelitian ini terdiri dari data transaksi digital yang mencakup berbagai jenis transaksi seperti pembayaran, pembelian e-commerce, dan transaksi pada platform peer-to-peer lending. Data tersebut mencakup fitur-fitur transaksi seperti jumlah transaksi, waktu transaksi, metode pembayaran, lokasi pengguna, dan berbagai informasi relevan lainnya. Untuk memastikan kualitas data, dataset akan dilabeli dengan dua kategori yaitu transaksi fraud (penipuan) dan non-fraud (bukan penipuan), serta dilakukan pembersihan data untuk menghilangkan data yang tidak lengkap atau tidak relevan. Data

kemudian dinormalisasi agar algoritma machine learning dapat memprosesnya dengan lebih optimal.

Selanjutnya, tahap penelitian ini berfokus pada implementasi algoritma machine learning yang telah dipilih untuk mendeteksi penipuan pada transaksi digital. Beberapa algoritma yang akan diujikan dalam penelitian ini antara lain Support Vector Machine (SVM), Random Forest, dan Ensemble Learning. Setiap algoritma akan diterapkan menggunakan bahasa pemrograman Python dan pustaka machine learning seperti scikit-learn. SVM dipilih karena kemampuannya dalam mengklasifikasikan data dengan baik meskipun dataset yang digunakan tidak seimbang (Eldo et al., 2024). Random Forest, yang merupakan algoritma ensemble learning, dipilih untuk mengidentifikasi pola transaksi fraud dengan menggabungkan banyak pohon keputusan dan meningkatkan akurasi deteksi penipuan (Kolbia & Dahliyanti, 2024). Sedangkan Ensemble Learning akan digunakan untuk menggabungkan beberapa model prediksi agar hasil deteksi penipuan dapat lebih akurat dan mengurangi risiko kesalahan (Saputra et al., 2024).

Selama proses implementasi, data latih (training data) akan digunakan untuk melatih model, sementara data uji (test data) akan digunakan untuk menguji performa algoritma. Metrik evaluasi yang digunakan untuk mengukur kinerja setiap algoritma mencakup akurasi, precision, recall, dan F1-score. Evaluasi ini penting untuk menilai seberapa baik algoritma dalam mengidentifikasi transaksi penipuan dan meminimalkan kesalahan, seperti false positives dan false negatives. Validasi silang (cross-validation) juga akan dilakukan untuk menguji stabilitas dan keandalan hasil model, dengan membagi dataset menjadi beberapa bagian dan melatih serta menguji model secara berulang dengan kombinasi data yang berbeda.

Setelah proses pengujian dan evaluasi selesai, tahap berikutnya adalah analisis hasil yang diperoleh. Hasil deteksi penipuan dari masing-masing algoritma akan dibandingkan dengan data transaksi yang diketahui sebagai fraud atau non-fraud untuk mengevaluasi keakuratan dan kehandalan setiap algoritma. Selain itu, penelitian ini akan membahas tantangan yang dihadapi dalam implementasi sistem deteksi penipuan berbasis machine learning, seperti masalah terkait dengan data yang tidak seimbang, overfitting, dan keterbatasan model dalam mendeteksi pola penipuan yang baru atau yang belum pernah ada sebelumnya. Selain itu, analisis juga akan mencakup pembahasan mengenai permasalahan privasi dan keamanan data pengguna yang harus diperhatikan dalam penerapan teknologi machine learning di sektor fintech dan e-commerce.

Secara keseluruhan, metode penelitian ini bertujuan untuk memberikan gambaran yang lebih komprehensif mengenai penerapan algoritma machine learning dalam mendeteksi

penipuan pada transaksi digital. Hasil yang diperoleh dari penelitian ini diharapkan dapat memberikan wawasan yang lebih dalam tentang efektivitas algoritma-algoritma tersebut dan memberikan rekomendasi mengenai algoritma mana yang lebih cocok digunakan untuk mendeteksi penipuan pada sektor fintech dan e-commerce. Penelitian ini juga diharapkan dapat memberikan kontribusi terhadap pengembangan sistem antifraud yang lebih efektif dan efisien dalam mengidentifikasi serta mencegah penipuan pada transaksi digital.

3. HASIL DAN PEMBAHASAN

Hasil dan pembahasan dalam penelitian ini bertujuan untuk memberikan wawasan mendalam mengenai efektivitas algoritma machine learning dan algoritma deteksi anomali dalam mendeteksi penipuan pada transaksi digital. Berdasarkan pengujian yang dilakukan terhadap beberapa algoritma machine learning seperti Support Vector Machine (SVM), Random Forest, dan Ensemble Learning, hasil yang diperoleh menunjukkan berbagai tingkat efektivitas dalam mendeteksi penipuan pada transaksi digital, terutama dalam konteks e-commerce dan fintech. Penelitian ini juga menganalisis tantangan yang dihadapi dalam penerapan sistem deteksi penipuan berbasis machine learning serta memberikan rekomendasi untuk meningkatkan kinerja dan efektivitas sistem tersebut.

Pada tahap pertama pengujian, algoritma Support Vector Machine (SVM) menunjukkan kinerja yang cukup baik dalam mengidentifikasi transaksi fraud. SVM bekerja dengan memetakan data dalam ruang dimensi yang lebih tinggi untuk menemukan hyperplane yang memisahkan kelas transaksi fraud dan non-fraud. Penggunaan SVM dalam penelitian ini terbukti efektif dalam menangani data yang tidak seimbang, di mana jumlah transaksi fraud jauh lebih sedikit dibandingkan dengan transaksi non-fraud. Hasil evaluasi menggunakan metrik akurasi, precision, recall, dan F1-score menunjukkan bahwa SVM memiliki tingkat recall yang tinggi, yang mengindikasikan kemampuannya dalam mendeteksi transaksi fraud meskipun jumlahnya terbatas. Namun, meskipun SVM menunjukkan kinerja yang baik, penelitian ini juga menemukan bahwa model ini rentan terhadap masalah overfitting ketika data yang digunakan sangat besar dan kompleks. Overfitting terjadi ketika model terlalu memfokuskan pada data latih sehingga kesulitan dalam generalisasi pada data uji yang tidak dikenal. Hal ini menunjukkan perlunya penyesuaian parameter dan pengaturan kernel pada SVM untuk meningkatkan akurasi dan kemampuan generalisasi model.

Selanjutnya, algoritma Random Forest, yang merupakan algoritma ensemble learning, juga diuji dalam penelitian ini. Random Forest membangun banyak pohon keputusan yang masing-masing melakukan klasifikasi berdasarkan subset data yang berbeda, kemudian

menggabungkan hasil dari semua pohon untuk menghasilkan keputusan akhir. Keunggulan utama dari Random Forest adalah kemampuannya dalam menangani data yang besar dan kompleks tanpa rentan terhadap overfitting, berkat penggunaan teknik bagging dan pemilihan acak fitur. Hasil pengujian menunjukkan bahwa Random Forest memiliki tingkat akurasi yang lebih tinggi dibandingkan dengan SVM dalam mendeteksi transaksi fraud. Metrik evaluasi menunjukkan bahwa Random Forest memiliki kombinasi akurasi, precision, dan recall yang lebih seimbang, yang membuatnya lebih handal dalam menangani transaksi yang tidak seimbang dan mendeteksi penipuan dengan lebih efektif. Salah satu alasan utama keberhasilan Random Forest adalah kemampuannya untuk menangani fitur-fitur yang tidak linier dengan baik, yang merupakan karakteristik umum pada transaksi digital yang melibatkan banyak variabel.

Namun, meskipun Random Forest menunjukkan hasil yang menjanjikan, tantangan utama yang dihadapi adalah kebutuhan akan sumber daya komputasi yang lebih besar, terutama dalam hal memori dan waktu komputasi ketika dataset yang digunakan sangat besar. Penelitian ini juga mencatat bahwa meskipun Random Forest dapat menangani data yang kompleks, algoritma ini masih bisa terpengaruh oleh data yang sangat tidak seimbang, di mana transaksi fraud yang lebih jarang mungkin tidak terdeteksi dengan optimal. Oleh karena itu, perlu dilakukan teknik penyeimbangan data, seperti oversampling pada data yang jarang, untuk meningkatkan kinerja algoritma.

Penerapan algoritma Ensemble Learning, yang menggabungkan hasil dari beberapa model untuk meningkatkan akurasi dan mengurangi kesalahan deteksi, juga diuji dalam penelitian ini. Ensemble Learning terbukti memberikan peningkatan yang signifikan dalam hal akurasi dan recall dibandingkan dengan penggunaan algoritma tunggal seperti SVM dan Random Forest. Salah satu metode yang digunakan dalam Ensemble Learning adalah teknik boosting, yang memungkinkan model untuk fokus pada kesalahan yang dilakukan oleh model sebelumnya, sehingga meningkatkan kemampuan prediksi pada transaksi yang sulit dideteksi. Hasil evaluasi menunjukkan bahwa Ensemble Learning memiliki akurasi yang lebih tinggi dan lebih stabil dalam mendeteksi transaksi fraud, dengan tingkat false positive yang lebih rendah. Hal ini menunjukkan bahwa dengan menggabungkan beberapa algoritma, Ensemble Learning dapat meminimalkan kelemahan yang ada pada masing-masing algoritma individu.

Namun, meskipun Ensemble Learning memberikan kinerja yang sangat baik, penelitian ini juga menunjukkan bahwa teknik ini memerlukan waktu komputasi yang lebih lama, terutama ketika menggabungkan banyak model yang berbeda. Selain itu, meskipun Ensemble Learning mampu meningkatkan kinerja dalam mendeteksi transaksi penipuan,

tantangan utama yang dihadapi adalah perlunya data yang lebih besar dan lebih berkualitas agar model dapat berfungsi secara optimal. Tanpa data yang cukup dan representatif, hasil yang diperoleh mungkin tidak akurat dan dapat menghasilkan false positives atau false negatives yang tinggi.

Selama proses pengujian dan evaluasi, penelitian ini juga memperhatikan masalah ketidakseimbangan data (imbalanced data), yang merupakan tantangan utama dalam deteksi penipuan pada transaksi digital. Transaksi fraud yang jauh lebih sedikit dibandingkan dengan transaksi non-fraud dapat menyebabkan model machine learning mengalami kesulitan dalam mempelajari pola penipuan yang ada. Untuk mengatasi hal ini, penelitian ini menggunakan teknik resampling seperti oversampling pada data fraud untuk meningkatkan representasi transaksi fraud dalam dataset. Teknik ini terbukti efektif dalam meningkatkan recall dan akurasi pada deteksi transaksi penipuan. Selain itu, penelitian ini juga menemukan bahwa penyesuaian threshold pada probabilitas deteksi dapat membantu meningkatkan kinerja model dalam mendeteksi transaksi fraud.

Meskipun hasil penelitian ini menunjukkan bahwa algoritma machine learning seperti SVM, Random Forest, dan Ensemble Learning dapat memberikan kontribusi signifikan dalam deteksi penipuan pada transaksi digital, terdapat beberapa tantangan yang perlu diatasi. Salah satu tantangan terbesar adalah masalah interpretabilitas model, di mana model machine learning yang lebih kompleks, seperti Random Forest dan Ensemble Learning, seringkali dianggap sebagai "black box" karena sulit untuk memahaminya secara intuitif. Hal ini dapat menjadi masalah dalam sektor fintech dan e-commerce, di mana keputusan yang diambil berdasarkan hasil model harus dapat dijelaskan secara transparan kepada pihak yang terlibat.

Selain itu, meskipun algoritma yang digunakan dalam penelitian ini menunjukkan hasil yang baik dalam mendeteksi penipuan, penelitian ini juga mencatat bahwa penipuan digital yang terus berkembang dapat memerlukan adaptasi model yang lebih cepat. Oleh karena itu, pengembangan sistem deteksi penipuan berbasis machine learning harus selalu disertai dengan pembaruan model secara berkala untuk memastikan bahwa sistem tetap efektif dalam menghadapi berbagai metode penipuan baru yang muncul.

Secara keseluruhan, penelitian ini menunjukkan bahwa penerapan machine learning, terutama algoritma SVM, Random Forest, dan Ensemble Learning, memiliki potensi besar dalam mendeteksi penipuan pada transaksi digital. Keberhasilan deteksi penipuan ini dapat meningkatkan keamanan dan kepercayaan pengguna dalam transaksi digital, yang sangat penting bagi pertumbuhan sektor fintech dan e-commerce. Namun, untuk mencapai hasil yang optimal, diperlukan penyesuaian algoritma, pemilihan model yang tepat, serta pengolahan data

yang baik untuk menangani tantangan yang dihadapi dalam deteksi penipuan berbasis machine learning.

4. KESIMPULAN

Kesimpulan dari penelitian ini menunjukkan bahwa penerapan machine learning, khususnya algoritma seperti Support Vector Machine (SVM), Random Forest, dan Ensemble Learning, memiliki potensi besar dalam mendeteksi penipuan pada transaksi digital, terutama dalam sektor fintech dan e-commerce. Masing-masing algoritma menunjukkan kelebihan dan kekurangan yang berbeda dalam hal akurasi, recall, dan kemampuan untuk menangani dataset yang tidak seimbang. SVM terbukti efektif dalam menangani data yang tidak seimbang, tetapi rentan terhadap masalah overfitting. Random Forest memberikan hasil yang lebih stabil dan lebih tinggi dalam hal akurasi serta recall, namun membutuhkan sumber daya komputasi yang lebih besar. Sementara itu, Ensemble Learning menunjukkan hasil yang lebih baik dalam meningkatkan akurasi deteksi penipuan dengan menggabungkan kekuatan beberapa model, meskipun memerlukan waktu komputasi yang lebih lama.

Masalah utama yang ditemukan dalam penelitian ini adalah ketidakseimbangan data, yang seringkali menjadi tantangan besar dalam deteksi penipuan. Data transaksi fraud yang lebih sedikit dibandingkan dengan transaksi non-fraud dapat memengaruhi kinerja model dalam mendeteksi pola penipuan. Oleh karena itu, teknik penyeimbangan data seperti oversampling terbukti efektif dalam meningkatkan performa model. Selain itu, meskipun algoritma machine learning yang digunakan dalam penelitian ini memberikan hasil yang memuaskan, tantangan seperti interpretabilitas model dan kebutuhan untuk pembaruan model secara berkala harus diatasi agar sistem deteksi penipuan tetap relevan dan efektif.

Penelitian ini juga menunjukkan bahwa penerapan algoritma machine learning dalam sistem antifraud dapat meningkatkan keamanan transaksi digital dan membangun kepercayaan pengguna. Namun, untuk mencapai hasil yang optimal, pengembangan lebih lanjut dalam hal teknik algoritma, pengolahan data, dan evaluasi model perlu dilakukan. Sistem deteksi penipuan berbasis machine learning harus dirancang dengan mempertimbangkan fleksibilitas dalam menghadapi berbagai jenis penipuan baru yang terus berkembang, serta memastikan bahwa hasil yang diberikan oleh model dapat dipahami dan diterima oleh pihak-pihak yang terlibat dalam pengambilan keputusan.

Secara keseluruhan, penelitian ini memberikan kontribusi signifikan terhadap pengembangan sistem deteksi penipuan berbasis machine learning di sektor fintech dan e-

commerce, serta membuka jalan bagi penelitian lebih lanjut untuk mengatasi tantangan yang ada dan memperbaiki kinerja sistem deteksi penipuan dalam transaksi digital.

5. 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.

Caseba, F. L., & Dewayanto, T. (2024). Penerapan artificial intelligence, big data, dan blockchain dalam fintech payment terhadap risiko penipuan komputer (computer fraud risk): A systematic literature review. *Diponegoro Journal of Accounting*, *13*(3).

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.

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.

Judijanto, L., Al-Amin, A. A., & Nurhakim, L. (2024). Implementasi Teknologi Artificial Intelligence dan Machine Learning dalam Praktik Akuntansi dan Audit: Sebuah Revolusi atau Evolusi. *COSMOS: Jurnal Ilmu Pendidikan, Ekonomi dan Teknologi*, *1*(6), 470-483.

Kolbia, U., & Dahliyanti, N. (2024). ANALISIS KECURANGAN DALAM MENGHADAPI PENIPUAN DI SITUS E-COMMERCE MENGGUNAKAN RANDOM FOREST; PENDEKATAN MACHINE LEARNING BERBASIS AI. *Jurnal Ilmiah Informatika Komputer*, *29*(2), 182-196.

Lubis, D. J., & Andri, A. N. R. (2024). Implementasi Algoritma Random Forest Untuk Optimasi Keamanan Autentikasi One-Time Password (OTP). *Informatech: Jurnal Ilmiah Informatika dan Komputer*, *1*(1), 23-29.

Mahya, L., Tarjo, T., Sanusi, Z. M., & Kurniawan, F. A. (2023). Intelligent Automation Of Fraud Detection And Investigation: A Bibliometric Analysis Approach. *Jurnal Reviu Akuntansi dan Keuangan*, *13*(3), 588-613.

Saputra, D. R. K., Via, Y. V., & Sihananto, A. N. (2024). Deteksi Anomali Menggunakan Ensemble Learning Dan Random Oversampling Pada Penipuan Transaksi Keuangan. *Jurnal Informatika dan Teknik Elektro Terapan*, *12*(3).

Valentino, M. R. (2023). Security Analysis Of AI-Based Mobile Application For Fraud. *Jurnal Komputer Indonesia*, *2*(1), 9-18.

Sutabri, Tata. (2012). Analisis Sistem Informasi. Yogyakarta: Penerbit Andi.

Sutabri, Tata dan Napitupulu, Darmawan. (2019). Sistem Informasi Bisnis.

Yogyakarta: Penerbit Andi.