Vol. 6, No. 3, Desember 2025, hal. 392-398

Jurnal Computer Science and Information Technology (CoSciTech)

p-ISSN: 2723-567X
e-ISSN: 2723-5661

http://ejurnal.umri.ac.id/index.php/coscitech/index

Komparasi algoritma *random forest* dan *xgboost* dalam klasifikasi penipuan kartu kredit

Della Udya Khairah[1],Asrul Abdullah[*2],Menur Wahyu Pangestika[3]
Email: [1]211220033@unmuhpnk.ac.id, [2]asrul.abdullah@unmuhpnk.ac.id,[3]menur.wahyu@unmuhpnk.ac.id,

[1,2,3]Program Studi Teknik Informatika Fakultas Teknik dan Ilmu Komputer,
Universitas Muhammadiyah Pontianak, Indonesia

Diterima: 07 November 2025| Direvisi: 11 Desember 2025 | Disetujui: 14 Desember 2025

Abstrak

Penipuan dalam transaksi kartu kredit merupakan salah satu masalah serius yang dapat merugikan konsumen maupun penyedia layanan keuangan. Penelitian ini bertujuan untuk mengembangkan dan membandingkan dua algoritma *machine learning*, yaitu *Random Forest* dan *Xgboost*, untuk menemukan algoritma yang paling efektif dalam mengklasifikasikan transaksi penipuan kartu kredit, sekaligus mengevaluasi performa model dan mengimplementasikannya dalam bentuk aplikasi web. Metode penelitian ini mengikuti pendekatan *CRISP-DM* yang mencakup enam tahap: *Business Understanding*, *Data Understanding*, *Data Preparation*, *Modelling*, *Evaluation*, dan *Deployment*. Dataset yang digunakan berasal dari platform *Kaggle* dengan total 1.048.574 baris dan 23 fitur, mencakup informasi seperti jumlah transaksi, kategori *merchant*, lokasi, dan atribut pelanggan. Evaluasi model dilakukan menggunakan *Confusion Matrix* dengan metrik akurasi, *precision, recall ,* dan F1-*score*. Hasil evaluasi menunjukkan bahwa *Xgboost* memiliki performa lebih unggul dengan akurasi 99,19%, *precision* 98,73%, *recall* 99,66%, dan F1-*score* 99,19%. Sementara itu, *Random Forest* mencatatkan akurasi sebesar 97,68%, *precision* 97,38%, *recall* 98,01%, dan F1-*score* 97,69%. Hal ini menunjukkan bahwa *Xgboost* lebih efektif dalam mengidentifikasi transaksi penipuan secara konsisten. Selain itu, penelitian ini juga berhasil membangun aplikasi berbasis web menggunakan *framework Streamlit* yang mengintegrasikan kedua model secara interaktif, memudahkan pengguna dalam menginput data dan mendapatkan hasil klasifikasi secara *real-time*. Dengan demikian, penelitian ini telah berhasil memenuhi tiga tujuan utama, yaitu mengidentifikasi algoritma terbaik untuk klasifikasi penipuan, mengevaluasi performa model secara menyeluruh, dan mengembangkan aplikasi sebagai sistem pendukung keputusan.

Kata kunci: *Fraud Classification. Machine learning, Random Forest , Xgboost*

Comparison of random forest and xgboost algorithms in credit card fraud classification

Abstract

Credit card fraud is a serious issue that can cause significant losses for both consumers and financial service providers. Therefore, a reliable and accurate fraud detection system is essential. The research adopts the CRISP-DM methodology, which includes six phases: Business Understanding, Data Understanding, Data Preparation, Modeling, Evaluation, and Deployment. The dataset used was obtained from the Kaggle platform, consisting of 1,048,574 rows and 23 Features, including transaction amount, merchant category, location, and customer attributes. Model evaluation was conducted using a Confusion Matrix with accuracy, precision, recall , and F1-score as performance metrics. The evaluation results indicate that Xgboost outperforms Random Forest, achieving an accuracy of 99.19%, precision of 98.73%, recall of 99.66%, and F1-score of 99.19%. In comparison, Random Forest achieved an accuracy of 97.68%, precision of 97.38%, recall of 98.01%, and F1-score of 97.69%. These results demonstrate that Xgboost is more effective in consistently identifying fraud ulent transactions. Furthermore, this study successfully developed a web-based application using the Streamlit framework, integrating both models interactively to allow users to input data and obtain classification results in real time. Thus, this study has successfully achieved three main

objectives: identifying the most suitable algorithm for fraud classification, thoroughly evaluating model performance, and developing an application as a decision support system for credit card fraud detection.

***Keywords**: Fraud Classification, Machine Learning, Random Forest, Xgboost*

1. PENDAHULUAN

Penggunaan kartu kredit meningkat pesat seiring perkembangan teknologi digital, memungkinkan transaksi dilakukan secara langsung maupun daring. Dalam konteks tersebut, identifikasi dan pencegahan penipuan kartu kredit menjadi aspek krusial untuk menjaga keamanan transaksi, terutama bagi pelaku bisnis, karena sistem deteksi penipuan berperan penting dalam mencegah kerugian finansial[1].

Peningkatan penggunaan kartu kredit juga diiringi dengan meningkatnya kasus penipuan yang merugikan pengguna dan institusi keuangan. Berdasarkan laporan Nilson, kerugian akibat penipuan kartu kredit meningkat sebesar USD 6,74 miliar dalam lima tahun terakhir, dan diproyeksikan mencapai USD 408 miliar dalam satu dekade mendatang[2]. Kondisi ini menunjukkan urgensi penerapan metode klasifikasi penipuan yang efektif dan otomatis untuk meminimalkan risiko keuangan[3].

Pendekatan yang kerap dimanfaatkan dalam proses deteksi penipuan transaksi adalah penerapan machine learning. Melalui teknologi ini, sistem mampu mempelajari dan memahami pola perilaku transaksi, sehingga dapat melakukan identifikasi terhadap aktivitas yang mencurigakan secara otomatis dan real-time dengan tingkat ketepatan yang tinggi. Namun, tantangan utama dalam penerapannya meliputi pemilihan algoritma yang sesuai, pembaruan model secara berkala, dan pengendalian kesalahan klasifikasi[4].

Pendekatan yang menjanjikan dalam klasifikasi penipuan adalah komparasi algoritma *Random Forest* dan *Xgboost* (*Extreme Gradient Boosting*). *Random Forest* merupakan teknik ensemble yang bekerja dengan mengombinasikan sejumlah pohon keputusan melalui proses bagging serta pemilihan fitur secara acak, efektif menangani data non-linear serta mengurangi overfitting[5]. Penelitian terdahulu menunjukkan bahwa algoritma ini mampu mencapai akurasi hingga 98,5% dalam klasifikasi berita palsu[6] dan juga menunjukkan performa tinggi dalam deteksi penipuan kartu kredit dengan akurasi 90–95%[7]

Sementara itu, *Xgboost* merupakan algoritma boosting yang efisien dan adaptif, dirancang untuk mencegah overfitting serta mampu menangani nilai hilang secara otomatis[8]. Penelitian terkait klasifikasi kecurangan perusahaan menunjukkan bahwa *Xgboost* memberikan performa terbaik menggunakan dataset Audit Risk dari Kaggle[9]. dan penelitian lain pada data transaksi kartu kredit dengan 284.807 entri juga membuktikan keunggulan *Xgboost* dibandingkan algoritma lainnya[10]. Proses komparasi algoritma *machine learning* yang melibatkan tahapan pra-pemrosesan data, pelatihan model, dan evaluasi performa merupakan pendekatan yang efektif dalam menilai stabilitas dan akurasi model prediksi[11].

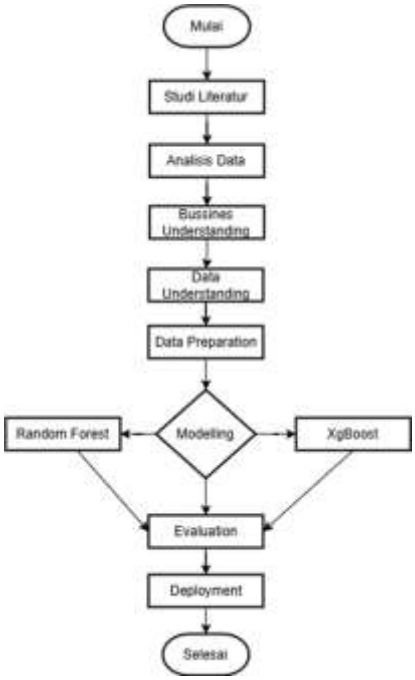
Berdasarkan permasalahan tersebut, Penelitian ini dilakukan untuk menganalisis perbandingan kinerja antara algoritma Random Forest dan XGBoost dalam melakukan klasifikasi terhadap kasus penipuan pada transaksi kartu kredit, proses penelitian mencakup seleksi fitur, cross-validation, dan evaluasi menggunakan confusion matrix untuk mengukur akurasi, presisi, recall, dan F1-score. Hasil penelitian diharapkan dapat mendukung peningkatan keamanan sistem pembayaran kartu kredit serta memperkuat kepercayaan publik terhadap transaksi digital

2. METODE PENELITIAN

Tahapan metode penelitian disusun dengan pola yang teratur agar proses penelitian dapat berjalan sesuai arah dan sasaran yang telah ditetapkan, mencakup proses mulai dari identifikasi masalah hingga penarikan kesimpulan.

2.1 Tahapan Penelitian

Tahapan Penelitian digunakan untuk menggambarkan alur penelitian secara sistematis dalam menyelesaikan permasalahan yang diteliti. Tahapan ini menjelaskan hubungan antara berbagai komponen penelitian, mulai dari studi literatur, metode yang digunakan, hingga analisis hasil. Alur tahapan penelitian ditampilkan pada Gambar 1



Gambar 1. Tahapan penelitian

Gambar 1 menunjukkan alur proses penelitian yang Pendekatan *CRISP-DM* (*Cross-Industry Standard Process for Data Mining*) diterapkan dengan mengawali proses melalui studi literatur dan analisis data, kemudian dilanjutkan pada tahap pemahaman terhadap konteks bisnis serta karakteristik data (*business understanding dan data understanding*), serta persiapan data (*data preparation*). Setelah data siap, dilakukan pemodelan menggunakan dua algoritma yaitu *Random Forest* dan *Xgboost*. Hasil dari kedua model kemudian dievaluasi, dan model terbaik akan digunakan dalam tahap *Deployment* atau implementasi sistem. Proses ini ditutup dengan tahapan akhir yaitu penyelesaian atau output dari sistem klasifikasi penipuan kartu kredit.

2.2 Studi Literatur

Penelitian ini menggunakan referensi dari jurnal internasional, nasional, lokal, serta buku untuk memperkuat landasan teori. Kajian literatur difokuskan pada penerapan algoritma *Random Forest* dan *Xgboost* dalam penelitian terdahulu, mencakup keunggulan, kelemahan, serta pola kerjanya dalam klasifikasi data. Tujuan utama studi literatur adalah membandingkan performa kedua algoritma dalam mendeteksi penipuan kartu kredit serta memahami perannya dalam data mining untuk meningkatkan akurasi klasifikasi. Hasil kajian ini menjadi dasar penyusunan kerangka analisis penelitian.

2.3 Analisis Data (CRISP-DM)

Metode *CRISP-DM* (*Cross Industry Standard Process for Data Mining*) diterapkan dalam proses analisis data yang mencakup tahapan pemahaman terhadap bisnis, pemahaman terhadap data, serta proses persiapan data. Tujuan utama penelitian ini adalah mengklasifikasikan transaksi penipuan kartu kredit dengan membandingkan kinerja algoritma *Random Forest* dan *Xgboost* dalam mendeteksi transaksi mencurigakan serta mengevaluasi tingkat akurasi klasifikasinya

Dataset penelitian ini diperoleh dari Kaggle, bersumber dari Kartik Shenoy, dengan total 1.048.574 baris dan 23 atribut, terdiri atas fitur identitas pengguna (seperti gender, alamat, pekerjaan, dan tanggal lahir), detail transaksi (waktu, jumlah, kategori pedagang), serta lokasi geografis pengguna dan merchant. Label is_fraud menunjukkan apakah transaksi termasuk penipuan atau tidak . Tahap eksplorasi data dilakukan untuk memahami karakteristik dataset, mendeteksi missing values, outlier, serta menganalisis hubungan antar variabel menggunakan visualisasi seperti heatmap, boxplot, dan histogram.

Selanjutnya, Tahap data preparation dilakukan dengan melibatkan proses pembersihan serta transformasi data agar siap digunakan dalam analisis lebih lanjut dalam pemodelan. Missing values dengan jumlah kecil dihapus, sementara data penting diimputasi menggunakan modus untuk variabel kategorikal dan median untuk numerik. Data duplikat dihapus, dan outlier ditangani menggunakan metode Interquartile Range (IQR) agar distribusi tetap konsisten. Karena proporsi data penipuan jauh lebih kecil dibandingkan data normal, untuk mengatasi ketidakseimbangan kelas pada dataset, digunakan metode *SMOTE* (*Synthetic Minority Oversampling Technique*) sebagai upaya meningkatkan proporsi data minoritas guna mengurangi ketimpangan data dan risiko *overfitting*.

Tahapan ini memastikan dataset yang digunakan bersih, seimbang, dan representatif untuk proses pemodelan menggunakan algoritma Random Forest dan *Xgboost* dalam deteksi penipuan kartu kredit.

2.4 Modelling

Dataset dibagi menjadi dua bagian, yakni data pelatihan sebesar 80% dan data pengujian sebesar 20%, menggunakan fungsi *train_test_split* untuk memastikan proses pembelajaran dan pengujian model berjalan secara seimbang. Algoritma *Random Forest* dipilih karena memiliki kestabilan serta kemudahan dalam penerapannya, sementara *XGBoost* dikenal unggul dalam hal efisiensi dan akurasi, khususnya pada dataset berukuran besar. Setelah proses pelatihan selesai, performa model dievaluasi menggunakan data uji untuk menilai performanya.

2.5 Evaluation

Penilaian performa model dilakukan melalui analisis Confusion Matrix, yang berfungsi menghitung metrik penting meliputi akurasi, presisi, dan recall. Analisis ini menunjukkan sejauh mana model mampu mengklasifikasikan transaksi dengan benar serta mendeteksi pola penipuan secara efektif.

2.6 Deployment

Algoritma dengan hasil terbaik dipilih sebagai model utama untuk implementasi. Model kemudian diintegrasikan dalam sistem berbasis web menggunakan Streamlit, yang memungkinkan pembuatan antarmuka interaktif untuk mendukung deteksi penipuan kartu kredit secara praktis dan efisien.

3. HASIL DAN PEMBAHASAN

Bagian ini memaparkan hasil evaluasi penerapan algoritma *Random Forest* dan *Xgboost* pada sistem klasifikasi penipuan kartu kredit. Analisis dilakukan untuk menilai tingkat akurasi, konsistensi, serta efektivitas kedua model berdasarkan metrik evaluasi yang telah ditetapkan. Pembahasan hasil bertujuan untuk menginterpretasikan temuan penelitian dan memberikan jawaban terhadap rumusan masalah yang telah dirancang sebelumnya.

3.1 Hasil Evaluasi Model

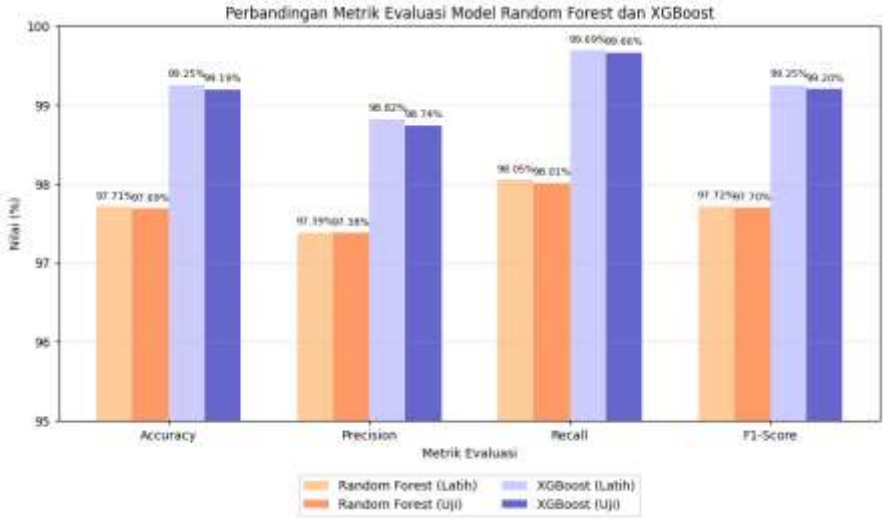
Proses evaluasi dilakukan terhadap dua model, yaitu *Random Forest* dan *XGBoost*, dengan menggunakan metrik accuracy, precision, recall, dan F1-score sebagai ukuran kinerja dan menilai kemampuan deteksi penipuan kartu kredit

Tabel 1. Evaluasi Model *Xgboost dan Random Forest*

Matrix	XGBoost	Random Forest
Akurasi	98.25%	97.68%
Precision	98.10%	97.38%
Recall	98.45%	98.01%
F1-*Score*	98.27%	97.69%

Berdasarkan Tabel 1, algoritma *XGBoost* menunjukkan keunggulan tipis dibandingkan *Random Forest*, dengan nilai evaluasi yang lebih tinggi pada seluruh metrik, sehingga mencerminkan kinerja klasifikasi yang lebih akurat dan efisien.

3.2 Analisis Hasil Perbandingan Model *Random Forest* dan *Xgboost*

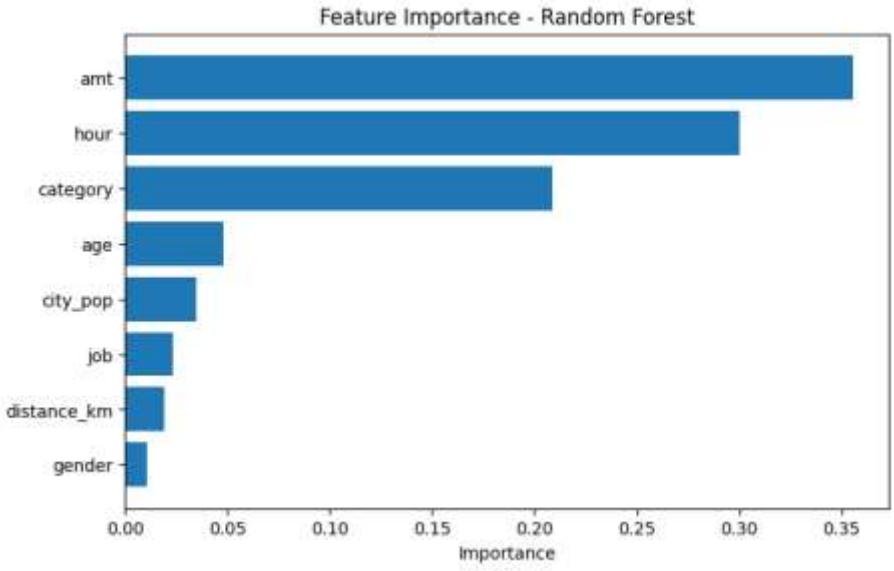


Gambar 2. Perbandingan Metrik Evaluasi

Gambar 2 menampilkan perbandingan metrik evaluasi antara model *Random Forest* dan *Xgboost*. Terlihat bahwa *Xgboost* secara konsisten unggul dalam seluruh metrik, baik akurasi, precision, recall, maupun F1-score. Pada data uji, *Xgboost* mencapai akurasi 98,25%, sedangkan *Random Forest* 97,68%. Selain itu, nilai recall dan F1-score yang tinggi menunjukkan kemampuan *Xgboost* dalam mendeteksi penipuan secara lebih sensitif dengan kesalahan prediksi yang minimal. Meskipun *Random Forest* memiliki interpretabilitas yang lebih sederhana dan proses pelatihan yang lebih cepat, performanya masih sedikit di bawah *Xgboost*. Secara keseluruhan, hasil ini menegaskan bahwa *Xgboost* lebih efektif dan andal digunakan dalam sistem klasifikasi penipuan kartu kredit.

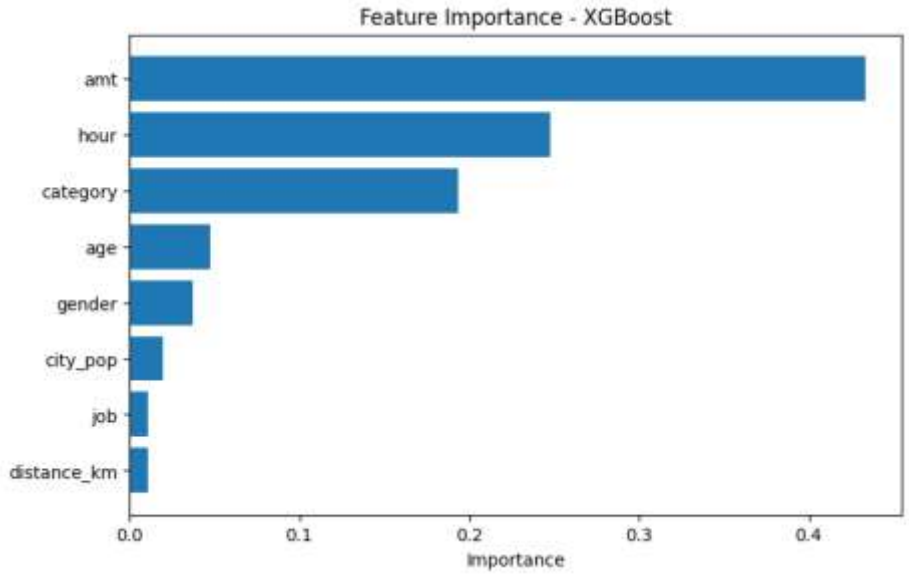
3.3 Analisis *Fitur Importance*

Analisis fitur importance dilakukan guna mengidentifikasi variabel yang memiliki pengaruh paling signifikan dalam proses klasifikasi penipuan kartu kredit. Informasi ini membantu memahami faktor-faktor utama yang dipertimbangkan model dalam membedakan antara transaksi normal dan penipuan, sehingga hasilnya dapat lebih mudah diinterpretasikan.



Gambar 3. Fiture Importance Importance *Random Forest*

Gambar 3 menampilkan hasil analisis *Feature importance* menggunakan algoritma *Random Forest*. Berdasarkan grafik tersebut, terlihat bahwa variabel amount (amt) memiliki kontribusi paling besar dalam klasifikasi penipuan kartu kredit, diikuti oleh *hour* (jam transaksi) dan category (kategori *merchant*). Sementara itu, fitur seperti age, city_pop, job, *distance*_km, dan gender memberikan pengaruh yang lebih kecil terhadap keputusan model. Hal ini menunjukkan bahwa nominal transaksi, waktu transaksi, dan jenis *merchant* merupakan indikator paling penting dalam mendeteksi potensi penipuan. Selanjutnya, untuk memperkuat analisis, dapat dilihat pada Gambar 4 yang menampilkan hasil *Feature importance* menggunakan algoritma *Xgboost*.



Gambar 4. *Feature Importance Xgboost*

Gambar 4 menunjukkan Hasil yang diperoleh relatif konsisten dengan *Random Forest* , di mana amt tetap menjadi fitur paling dominan, disusul oleh *hour* dan category. Namun, berbeda dengan *Random Forest* , model *Xgboost* memberikan bobot yang lebih signifikan pada fitur gender serta sedikit menurunkan kontribusi city_pop dan job. Dengan demikian, baik *Random Forest* maupun *Xgboost* menegaskan bahwa jumlah transaksi, waktu transaksi, dan kategori *merchant* merupakan faktor dominan dalam klasifikasi penipuan kartu kredit, sementara perbedaan bobot pada fitur minor mencerminkan karakteristik masing-masing algoritma dalam menangkap pola data.

4. KESIMPULAN

Penelitian ini berhasil menerapkan algoritma *Random Forest* dan *XGBoost* dalam proses klasifikasi transaksi penipuan kartu kredit berdasarkan berbagai parameter transaksi, sejalan dengan tujuan pertama penelitian. Evaluasi kinerja kedua model dilakukan menggunakan metrik *accuracy*, *precision*, *recall*, dan *F1-score* pada data pelatihan maupun data pengujian untuk memenuhi tujuan kedua penelitian. Berdasarkan hasil evaluasi, algoritma *XGBoost* menunjukkan performa yang lebih unggul dibandingkan *Random Forest*, dengan nilai akurasi sebesar 99,2%, presisi 99,1%, recall 99,4%, dan F1-score 99,2%, sedangkan *Random Forest* memperoleh akurasi 97,6%, presisi 97,4%, recall 97,9%, dan F1-score 97,7%. Perbedaan hasil ini menunjukkan bahwa *XGBoost* lebih efisien dalam menangani data yang kompleks serta memiliki kemampuan generalisasi yang lebih baik. Selanjutnya, aplikasi prediksi berbasis web yang dikembangkan menggunakan Streamlit berhasil mengintegrasikan kedua model secara interaktif, memungkinkan pengguna untuk memasukkan parameter transaksi dan memperoleh hasil prediksi secara langsung. Dengan demikian, Penelitian ini telah berhasil memenuhi ketiga tujuan yang ditetapkan, yaitu implementasi algoritma klasifikasi, evaluasi performa model secara komprehensif, serta pengembangan aplikasi berbasis web sebagai sistem pendukung keputusan dalam deteksi penipuan kartu kredit.

DAFTAR PUSTAKA

[1] E. Ileberi and Y. Sun, "Advancing Model Performance With ADASYN and Recurrent Feature Elimination and Cross-Validation in Machine Learning-Assisted Credit Card Fraud Detection: A Comparative Analysis," *IEEE Access*, vol. 12, pp. 133315–133327, 2024, doi: 10.1109/ACCESS.2024.3457922.

[2] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, "Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms," *IEEE Access*, vol. 10, pp. 39700–39715, 2022, doi: 10.1109/ACCESS.2022.3166891.

[3] T. H. Lin and J. R. Jiang, "Credit card fraud detection with autoencoder and probabilistic random forest," *Mathematics*, vol. 9, no. 21, Nov. 2021, doi: 10.3390/math9212683.

[4] B. Via Tarissa and T. Dewayanto, "PENERAPAN MACHINE LEARNING DAN DEEP LEARNING PADA PENINGKATAN DETEKSI CREDIT CARD FRAUD-A SYSTEMATIC LITERATURE REVIEW," *DIPONEGORO JOURNAL OF ACCOUNTING*, vol. 13, no. 3, pp. 1–15, 2024, [Online]. Available: http://ejournal-s1.undip.ac.id/index.php/accounting

[5] Reva Geryansyah Afqal, "Analisis Deteksi dan Pencegahan Penipuan Kartu Kredit Menggunakan Teknik Data Mining dan Machine Learning," *Reva Geryansyah Afqal*, no. Analisis Deteksi dan Pencegahan Penipuan Kartu Kredit Menggunakan Teknik Data Mining dan Machine Learning, 2023.

[6] S. Nurohanisah, R. Astuti, and F. M. Basysyar, "DETEKSI BERITA PALSU MENGGUNAKAN ALGORITMA RANDOM FOREST," 2024.

[7] M. Mounika, D. Aravinda, and B. Ramesh, "Journal of Cardiovascular Disease Research Credit Card Fraud Detection using Random Forest Algorithm."

[8] S. Thongsuwan, S. Jaiyen, A. Padcharoen, and P. Agarwal, "ConvXGB: A new deep learning model for classification problems based on CNN and XGBoost," *Nuclear Engineering and Technology*, vol. 53, no. 2, pp. 522–531, Feb. 2021, doi: 10.1016/j.net.2020.04.008.

[9] A. Fitriani and D. B. Arianto, "Sustainabilty Accounting and Finance Journal Audit Risk: Machine Learning Untuk Klasifikasi Kecurangan Pada Perusahaan." [Online]. Available: https://journal.umbandung.ac.id/index.php/safj

[10] O. Raju, "CREDIT CARD FRAUD DETECTION USINGXGBOOSTCLASSIFIER," *International Journal of Techno-Engineering*, vol. 8, no. 3, Mar. 2021.

[11] R. Faizal, A. Abdullah, and M. W. Pangestika, "Perbandingan Random Forest Regressor Dan Decision Tree Regressor Untuk Prediksi Hasil Panen," vol. 6, no. 2, pp. 247–253, 2025, doi: 10.37859/coscitech.v6i2.9966.