

DETEKSI PENIPUAN KARTU KREDIT MENGGUNAKAN METODE *RANDOM FOREST*

Khaerunni Salsa Billah¹⁾, Rizal Adi Saputra²⁾

^{1,2} Fakultas Teknik, Universitas Halu Oleo, Kendari

E-mail : ¹khaerunnisalsabillah22062@gmail.com, ²rizaladisaputra@gmail.com

Abstract

The increasing use of credit cards in Indonesia has raised concerns about the potential for fraud in these transactions. Data from Bank Indonesia shows that the number of credit cards in circulation in August 2023 reached 17.69 million, with transaction volume reaching 28,360 transactions as of May 2022. The high transaction volume and fast processing speed make manual monitoring impossible. Therefore, automatic monitoring is needed to prevent fraud in credit card transactions. This research aims to develop a machine learning-based credit card transaction fraud detection system using the Random Forest algorithm. Random Forest is used for classification, regression, and other tasks. A credit card transaction dataset from 2023 consisting of more than 550,000 data was used in this research. The research results show that of the total 568,630 records in the dataset, there were 113,726 records that were detected as fraudulent based on the classification model used. Through Random Forest analysis, features V4, V11, V22, V21, and V27 were identified as the most influential in detecting fraud. The developed model shows an accuracy rate of around 96.53%, supported by the roc_auc_score method which categorizes it as very good.

Keywords: Credit Card Detection, Fraud, Machine learning, Random Forest

Abstrak

Meningkatnya penggunaan kartu kredit di Indonesia menimbulkan kekhawatiran mengenai potensi penipuan dalam transaksi tersebut. Data dari Bank Indonesia menunjukkan bahwa jumlah kartu kredit yang beredar pada Agustus 2023 mencapai 17,69 juta, dengan volume transaksi mencapai 28.360 transaksi per Mei 2022. Volume transaksi yang tinggi dan kecepatan pemrosesan yang cepat membuat pengawasan manual tidak memungkinkan. Oleh karena itu, diperlukan pengawasan otomatis untuk mencegah tindak penipuan dalam transaksi kartu kredit. Penelitian ini bertujuan mengembangkan sistem pendeteksi penipuan transaksi kartu kredit berbasis *Machine learning* dengan menggunakan algoritma *Random Forest*. *Random Forest* digunakan untuk klasifikasi, regresi, dan tugas-tugas lainnya. *Dataeset* transaksi kartu kredit dari tahun 2023 yang terdiri lebih dari 550.000 data digunakan dalam penelitian ini. Hasil penelitian menunjukkan bahwa dari total 568.630 record dalam dataset, terdapat sejumlah 113.726 record yang terdeteksi sebagai penipuan berdasarkan model klasifikasi yang digunakan. Melalui analisis *Random Forest*, fitur V4, V11, V22, V21, dan V27 diidentifikasi sebagai yang paling berpengaruh dalam mendeteksi penipuan. Model yang dikembangkan menunjukkan tingkat akurasi sekitar 96,53%, didukung oleh metode *roc_auc_score* yang mengkategorikannya sebagai sangat baik.

Kata Kunci: Deteksi Kartu Kredit, Penipuan, *Machine learning*, *Random Forest*

1. PENDAHULUAN

Pertumbuhan teknologi informasi dan kemajuan dalam sistem keuangan modern telah membawa manfaat yang signifikan bagi masyarakat. Namun, kemajuan ini juga membuka peluang baru bagi berbagai jenis kejahatan keuangan, termasuk penipuan kartu kredit. Perkembangan ekonomi yang cepat menuntut terjadinya transaksi keuangan secara berlanjut, menjadikan pembayaran tunai dianggap sebagai metode yang ketinggalan zaman. Terlebih lagi, dengan munculnya sarana jual-beli

<https://doi.org/10.35145/joisie.v8i2.4064>

JOISIE licensed under a Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0)

dan transaksi *online* saat ini, perilaku konsumen dan bisnis menjadi lebih praktis dan instan (Hendarsyah et al., 2020). Kemudahan akses informasi dapat meningkatkan risiko penyalahgunaan informasi, terutama dalam tindak kejahatan seperti penipuan, penyerangan, dan berbagai kasus lainnya (Pourhabibi et al., 2020). Salah satu bentuk manipulasi data dalam bidang *e-commerce* adalah penipuan kartu kredit (Dornadula & Geetha, 2019). Kartu kredit adalah alat pembayaran yang memanfaatkan layanan dari bank atau perusahaan tertentu untuk melakukan transaksi jual beli, baik untuk membeli barang maupun mendapatkan jasa (Armiani & Agustini, 2022). Saat ini, terdapat beragam cara untuk melakukan cicilan, salah satunya adalah dengan menggunakan Visa atau kartu kredit (Batubara et al., 2022). Banyak masyarakat memilih menggunakan kartu kredit karena berbagai keuntungan yang ditawarkan. Salah satu keuntungan utamanya adalah pemilik kartu kredit dapat melakukan transaksi tanpa perlu membawa uang tunai. Selain itu, penerbit dan penyedia layanan kartu kredit seringkali memberikan berbagai penawaran menarik, seperti hadiah untuk pemegang kartu yang aktif bertransaksi, penawaran pinjaman jangka pendek tanpa bunga dengan syarat tertentu, serta jaminan transaksi yang andal dan nyaman. Faktor-faktor ini membuat masyarakat semakin tertarik untuk menggunakan kartu kredit dalam kegiatan finansial mereka.

Namun, seiring dengan meningkatnya penggunaan kartu kredit, tindak penipuan kartu kredit pun ikut meningkat sehingga dapat menyebabkan kerugian keuangan yang tidak sedikit (Ambarwati, 2020). Pada akhir tahun 2013, Asosiasi Kartu Kredit Indonesia (AKKI) mencatat bahwa jumlah kartu kredit yang beredar telah mencapai 15.007.492. Angka ini menunjukkan bahwa penggunaan kartu kredit di Indonesia berkembang sangat pesat (Alhamdani et al., 2021). Kemudian pada tahun 2020, berdasarkan data Asosiasi Kartu Kredit Indonesia (AKKI), pengguna kartu kredit mengalami peningkatan dengan jumlah mencapai 16.940.040. Berdasarkan data Statistik Sistem Pembayaran dan Infrastruktur Pasar Keuangan (SPIP) yang diterbitkan oleh Bank Indonesia pada Juni 2022, terlihat bahwa jumlah kartu kredit yang beredar di Indonesia mengalami peningkatan signifikan selama 10 tahun terakhir. Pada bulan Mei 2022, jumlah kartu kredit yang beredar mencapai 16.588.263 unit, meningkat sekitar 2 juta unit dibandingkan dengan jumlah pada tahun 2012 yang sebanyak 14.817.168 unit. Kemudian, data terbaru dari BI, jumlah kartu kredit pada Agustus 2023 mencapai 17.69 Juta, yang membuktikan pertumbuhan pengguna kartu kredit terus meningkat. Sementara itu, volume transaksi menggunakan kartu kredit di Indonesia pada bulan Mei 2022 mencapai 28.360 transaksi, menunjukkan peningkatan signifikan dibandingkan dengan volume transaksi pada Mei 2021 yang berjumlah 23.452 transaksi. Data ini mencerminkan pertumbuhan penggunaan kartu kredit dalam melakukan transaksi keuangan di Indonesia selama periode tersebut (Ningsih et al., 2022).

Data dari Cifa menunjukkan bahwa sebanyak 33.305 kasus penipuan kartu dilaporkan antara bulan Januari dan Juni 2018 (Sitohang et al., 2021). Sistem tidak dapat mengklasifikasikan sebuah transaksi secara definitif sebagai penipuan atau transaksi asli. Sistem hanya mendeteksi kemiripan dan kemungkinan transaksi sebagai penipuan berdasarkan analisis mendalam terhadap perilaku pelanggan, kebiasaan belanja, dan pola dari penipuan sebelumnya. Pola-pola ini digunakan untuk mengidentifikasi potensi penipuan (Jain, 2019). Tingginya angka penipuan kartu kredit menyebabkan peningkatan jumlah kasus yang terjadi dan memberikan tantangan dalam upaya pencegahannya (Febriady et al., 2022). Menurut laporan *World Economic Forum*, serangan *cyber* masuk dalam lima ancaman utama yang mengancam umat manusia, sejajar dengan bencana alam dan perubahan iklim. Kejahatan dunia maya, yang fokus utamanya adalah merampas properti, termasuk pencurian aset dari rekening bank, memiliki risiko khusus (Apriwandi. Herycson, 2022). Dengan demikian, deteksi penipuan kartu kredit sejak dini menjadi suatu keharusan. Dari total transaksi menggunakan kartu pada tahun 2019 yang mencapai 42.275 triliun dolar (mengalami peningkatan sebesar 4,2% dari tahun 2018), tercatat kerugian sebesar 28,65 miliar dolar (naik 2,9% dari tahun 2018) (Kurniawan & Yulianingsih, 2021). Menurut statistik, Indonesia menempati peringkat kedua dalam tingkat penipuan kartu kredit, mencapai 18,3% (Kumar Manjhvar & Goyal, 2020).

Penipuan ini memiliki dampak negatif bagi pemilik kartu kredit dan lembaga keuangan terkait, sehingga perlu dilakukan upaya untuk mengidentifikasi dan mencegah transaksi ilegal yang melibatkan kartu kredit. Oleh karena itu, diperlukan metode alternatif untuk mencegah penipuan transaksi kartu kredit, seperti melakukan deteksi sedini mungkin terhadap transaksi yang berlangsung. Namun, dengan tingginya volume transaksi dan kecepatan proses yang terus-menerus, melakukan

deteksi secara manual oleh manusia menjadi sangat tidak mungkin. Solusinya adalah dengan mengembangkan sebuah sistem pendeteksi penipuan transaksi kartu kredit, yaitu sistem yang dapat secara otomatis, cepat, akurat, dan berkelanjutan mendeteksi tindakan penipuan dalam transaksi kartu kredit tanpa keterlibatan manusia secara langsung. Pendekatan ini menggunakan teknik pembelajaran mesin (*machine learning*) (Diana et al., 2023). dan algoritma yang sesuai untuk mencapai tujuan tersebut (Werdiningsih et al., 2023). *Machine learning* adalah bagian dari kecerdasan buatan yang menggunakan kecepatan komputasi tinggi dan teknik pengenalan pola untuk menganalisis data dan menghasilkan pengetahuan baru. (Megalooikonomou & Beligiannis, 2023) Penyelesaian masalah klasifikasi dan prediksi menggunakan *machine learning* saat ini menjadi acuan yang dapat diandalkan karena mampu memberikan akurasi tinggi dalam menangani berbagai permasalahan (Afriyie et al., 2023).

Pada saat ini, *Machine learning* telah menjadi sangat umum digunakan dalam *data mining* dan *analisis big data*. Dalam konteks ini, pendekatan *Random Forest* (RF), yang merupakan bagian dari algoritma *supervised learning* dalam *Machine learning*, diterapkan dalam penelitian ini untuk memberikan solusi terbaik dalam menangani permasalahan deteksi penipuan (Lestari & Sirodj, 2022). Beberapa metode yang telah dikembangkan untuk mendeteksi keabsahan transaksi kartu kredit telah ada sejak lama (Carcillo et al., 2021). *Random Forest* adalah algoritma *machine learning* yang terdiri dari kombinasi beberapa pohon keputusan untuk membentuk sebuah "hutan" dari pohon keputusan. Algoritma ini bekerja dengan prinsip "kebijaksanaan kerumunan," dimana setiap pohon memberikan prediksi, dan hasil akhir ditentukan oleh mayoritas prediksi dari semua pohon. Keunggulan utama dari *Random Forest* adalah kemampuannya dalam mengatasi *overfitting* yang sering terjadi pada algoritma pohon keputusan tunggal, serta kemampuannya dalam menangani data yang kompleks dan variatif (Fadli & Saputra, 2023). Algoritma ini juga efektif dalam menangani dataset yang besar dengan banyak fitur dan dapat memberikan estimasi mengenai fitur-fitur yang paling penting dalam klasifikasi.

Keterbaruan dari penelitian ini terletak pada implementasi algoritma *Random Forest* yang dikombinasikan dengan teknik *praproses data* terbaru dan penyesuaian parameter yang optimal untuk mendeteksi penipuan kartu kredit dalam skala besar. Penelitian ini juga memanfaatkan dataset terbaru dan lebih besar dibandingkan penelitian sebelumnya, memungkinkan analisis yang lebih komprehensif dan akurat. Selain itu, penelitian ini mengintegrasikan metode validasi silang (*cross-validation*) yang lebih canggih untuk memastikan keandalan dan generalisasi model dalam berbagai skenario transaksi. Dengan demikian, penelitian ini tidak hanya menawarkan solusi deteksi penipuan yang lebih efektif, tetapi juga memberikan kontribusi signifikan dalam pengembangan metodologi *machine learning* dalam konteks keamanan keuangan.

2. METODE PENELITIAN

Random Forest digunakan sebagai metode untuk memprediksi mayoritas keberadaan penipuan dalam transaksi penggunaan kartu kredit. Selanjutnya, digunakan rumus untuk menghitung akurasi dalam konteks evaluasi model yang dirumuskan sebagai berikut:

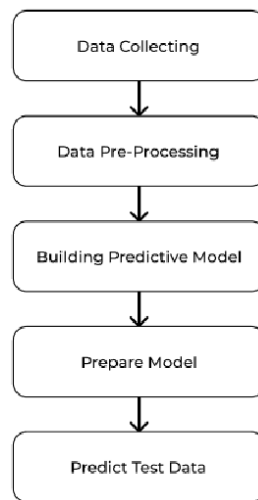
$$\text{Akurasi} = \frac{TP+TN}{TP+FP+TN+FN} \quad (1)$$

TP (*True Positive*) merupakan jumlah *instance* positif yang benar-benar diklasifikasikan dengan benar sebagai positif oleh model, sedangkan TN (*True Negative*) merupakan jumlah *instance* negatif yang benar-benar diklasifikasikan dengan benar sebagai negatif oleh model. FP (*False Positive*) merupakan jumlah *instance* negatif yang salah diklasifikasikan sebagai positif oleh model, dan terakhir FN (*False Negative*) merupakan jumlah *instance* positif yang salah diklasifikasikan sebagai negatif oleh model.

Data yang mendukung penelitian ini diperoleh dari Kaggle, dengan 31 variabel pengukuran. Dari 31 variabel tersebut, 29 variabel mencerminkan pola transaksi, termasuk informasi tentang waktu,

lokasi, dan sebagainya. Sementara itu, 2 variabel lainnya mencakup ID dan jumlah transaksi yang dimiliki oleh setiap nasabah kartu kredit. Keseluruhan, terdapat 568.631 data dalam *dataset* ini.

2.1 LANGKAH PENELITIAN



Gambar 1. Langkah Penelitian

Gambar 1 mengilustrasikan langkah-langkah penelitian untuk memprediksi kecurangan (*Fraud*) dengan membangun model menggunakan algoritma *Random Forest* dalam bahasa pemrograman Python:

- 1) *Data Collecting*: Langkah awal dalam penelitian ini adalah Pengumpulan data, yang melibatkan perolehan data yang relevan dan diperlukan. Sumber data berasal dari Kaggle dengan 31 variabel pengukuran. Dari 31 variabel tersebut, 29 diantaranya mencerminkan pola transaksi seperti informasi terkait waktu, lokasi, dan sebagainya. Sedangkan 2 lainnya merupakan ID dan jumlah transaksi tiap nasabah. Terdapat 568.631 data dalam *dataset* ini.
- 2) *Data Pre-Processing*: *Pre-processing* dianggap sebagai langkah yang penting untuk mendapatkan model klasifikasi dengan kinerja tinggi dalam prediksi (Alsarhan et al., 2021). *Dataset* akan melalui tahap *Pre-Processing* (Triyanto et al., 2021). *Data Pre-Processing* adalah langkah yang dilakukan pada data mentah sebelum digunakan dalam analisis. Dalam penelitian ini, dilakukan *Data Pre-Processing* dengan cara menampilkan informasi terkait data seperti jumlah baris, kolom, tipe data, dll. Setelah itu, dilakukan pengecekan apakah dalam data terdapat nilai yang hilang. Kemudian, dilakukan *Handling Missing Value* yaitu penanganan nilai yang hilang.
- 3) *Building Predictive Model*: Pembangunan Model Prediktif dalam penelitian ini menggunakan model regresi logistik.
- 4) *Prepare Model*: Model regresi logistik telah dilatih dan siap digunakan untuk memprediksi data baru.
- 5) *Predict Test Data*: Model regresi logistik digunakan untuk memprediksi data uji, kemudian hasil prediksi dievaluasi menggunakan *Confusion Matrix*.

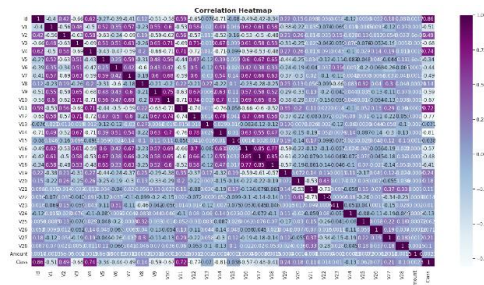
2.2 RANDOM FOREST

Random Forest merupakan pengembangan dari metode CART (*Classification and Regression Trees*) (Chairunisa et al., 2020), di mana analisis dilakukan pada n observasi dan p variabel penjelas. Proses ini melibatkan dua tahap utama, yaitu *bootstrap* dan pemilihan fitur acak, yang diulang sebanyak k kali untuk membentuk sebuah hutan terdiri dari k pohon. Peningkatan signifikan dalam kinerja prediksi tercapai melalui hasil pertumbuhan sekelompok pohon dan pemilihan kelas yang paling umum. Pada tahap *bootstrap*, penting untuk memastikan ukuran data yang digunakan cukup

besar, tidak memiliki banyak *outlier*, dan bukan data *time series*. Dengan konsep ini, *Random Forest* terbukti efektif dalam menangani berbagai jenis *dataset*.

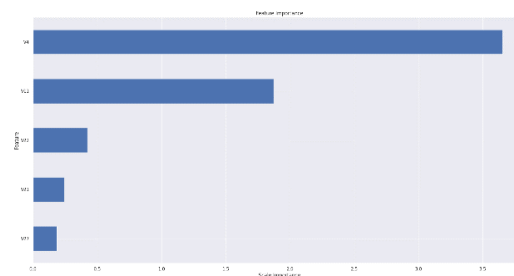
3. HASIL DAN PEMBAHASAN

Correlation map (heatmap) adalah representasi visual dari matriks korelasi antar-variabel dalam suatu *dataset*. Matriks korelasi mengukur sejauh mana dua variabel berkorelasi satu sama lain. Nilai korelasi berkisar antara -1 hingga 1, di mana 1 menunjukkan korelasi positif sempurna, -1 menunjukkan korelasi negatif sempurna, dan nilai 0 menunjukkan tidak adanya korelasi antara dua variabel tersebut. *Heatmap* memberikan gambaran visual yang jelas dan intuitif tentang hubungan antar-variabel dalam *dataset*, di mana warna yang berbeda menggambarkan tingkat korelasi yang berbeda, membantu analisis dan pemahaman hubungan antar-variabel dengan lebih mudah.



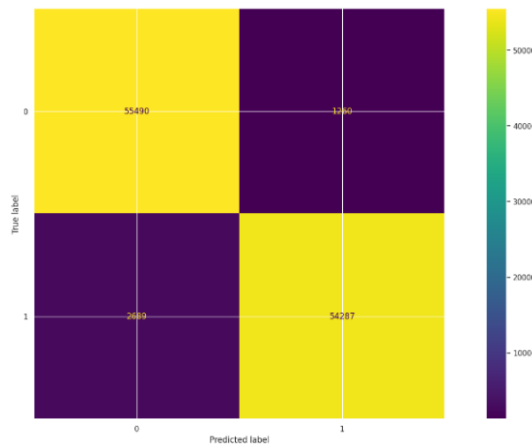
Gambar 2. *Correlation Map*

Dari gambar 2, semakin gelap warnanya menandakan semakin mendekati angka 1.0, yang berarti nilai korelasinya semakin mendekati positif sempurna. Dari 31 field data atau fitur yang digunakan, penting untuk menentukan fitur mana yang paling relevan atau memiliki pengaruh paling signifikan terhadap hasil prediksi. Hal ini memungkinkan kita untuk mengetahui prioritas langkah yang harus diambil dalam menyelesaikan masalah atau melakukan tindakan lebih lanjut. Hasil perhitungan ini dapat diperoleh melalui metode *Random Forest Built-in Feature Importance*.



Gambar 3. *Feature Importance*

Dari hasil grafik Gambar 3 mengenai *Feature Importance*, dapat disimpulkan bahwa fitur V4, V11, V22, V21, dan V27 merupakan unsur data yang memiliki pengaruh paling signifikan terhadap hasil prediksi. Dengan model yang digunakan, kita dapat memvisualisasikan hasil pengujian akurasi melalui visualisasi *Confusion Matrix*, seperti yang ditunjukkan dalam gambar berikut:

Gambar 4. *Confusion matrix* dari model klasifikasi

Dari hasil grafik pada Gambar 4, dapat disimpulkan bahwa model memiliki kinerja yang memadai dalam mengklasifikasikan data. Jumlah *True Negative* yang mencapai sekitar 55.000 menunjukkan kemampuan model dalam memprediksi dengan tepat transaksi yang bukan merupakan penipuan. Namun, terdapat sejumlah *False Positive* sebanyak 1.260 kali, yang mengindikasikan adanya transaksi yang salah diklasifikasikan sebagai penipuan. Selain itu, jumlah *False Negative* sebanyak 2.689 kali menunjukkan adanya kasus transaksi penipuan yang tidak berhasil terdeteksi oleh model. Meskipun demikian, jumlah *True Positive* yang mencapai 54.287 kali menunjukkan bahwa model dapat dengan efektif mengidentifikasi transaksi penipuan. Informasi dari *Confusion Matrix* ini penting untuk mengevaluasi secara holistik kualitas dan kehandalan model dalam tugas deteksi penipuan. Rumus-rumus yang dapat digunakan untuk evaluasi lebih lanjut adalah sebagai berikut:

$$\text{Akurasi} = \frac{TP+TN}{TP+FP+TN+FN} \quad (1)$$

$$\text{Akurasi} = \frac{54.287+55.000}{54.287+55.000+1.260+2.689} \quad (2)$$

$$\text{Akurasi} = \frac{109.287}{113.236} \quad (3)$$

$$\text{Akurasi} = 0.9653 \quad (4)$$

Dari *Confusion Matrix* tersebut, menghasilkan table berikut:

Tabel 1. *Classification Report*

	presisi	recall	f1-s	sup
0	0.9538	0.9778	0.9656	56750
1	0.9773	0.9528	0.9649	56976
accuracy			0.9653	113726
macro	0.9655		0.9653	113726
avg		0.9653		113726
weighted	0.9656		0.9653	113726
avg		0.9653		113726

Laporan klasifikasi menunjukkan bahwa model memiliki kinerja yang baik dengan akurasi keseluruhan sebesar 96,53%. Presisi dan *recall* seimbang untuk kedua kelas, dengan *F1-score* sebesar 96,56% untuk kelas 0 dan 96,49% untuk kelas 1. Berdasarkan perhitungan nilai prediksi menggunakan metode *roc_auc_score*, diperoleh nilai akurasi model sebesar 0.96. Hasil ini menunjukkan bahwa model yang digunakan memiliki tingkat akurasi yang tinggi, mencapai 96%. Dengan nilai akurasi

yang signifikan tersebut, dapat disimpulkan bahwa model tersebut cukup baik dalam mendeteksi kemungkinan tindak pidana penipuan kartu kredit.

Hasil penelitian menunjukkan bahwa dari total 568.630 record dalam dataset, terdapat sejumlah 113.726 record yang terdeteksi sebagai penipuan berdasarkan model klasifikasi yang digunakan. Keberhasilan model dalam memberikan prediksi yang akurat dapat memberikan keyakinan bahwa model ini efektif dalam membedakan antara transaksi yang sah dan yang berpotensi penipuan, sehingga berkontribusi positif dalam upaya keamanan dan perlindungan terhadap pengguna kartu kredit.

Tabel 2. Nilai akurasi

Rentang	Kategori
0.90-1.00	<i>Excellent classifications</i> (sangat baik)
0.80-0.90	<i>Good classifications</i> (baik)
0.70-0.80	<i>Fair classifications</i> (cukup)
0.60-0.70	<i>Poor classifications</i> (buruk)
0.5-0.60	<i>Failure</i> (gagal)

4. SIMPULAN

Berdasarkan serangkaian pengujian terhadap model yang dikembangkan menggunakan algoritma *Random Forest Classification*, diperoleh kesimpulan bahwa fitur yang paling relevan adalah V4. Hal ini diperkuat melalui visualisasi akurasi menggunakan *confusion matrix* dan perhitungan akurasi yang menghasilkan nilai sebesar 0.96 atau 96,53%, yang dapat dikategorikan sebagai sangat baik. Dengan demikian, dapat disimpulkan bahwa algoritma *Random Forest Classifier* dengan model yang telah dikembangkan mampu memberikan hasil yang sangat baik dalam mendeteksi penipuan kartu kredit. Hasil penelitian menunjukkan bahwa dari total 568.630 *record* dalam *dataset*, terdapat sejumlah 113.726 *record* yang terdeteksi sebagai penipuan berdasarkan model klasifikasi yang digunakan.

Keberhasilan ini menunjukkan kemampuan model dalam mengidentifikasi pola-pola yang mencurigakan atau tidak biasa dalam data transaksi keuangan, khususnya terkait dengan fitur yang paling relevan, yaitu V4. Ini menjadi langkah positif dalam mengamankan transaksi kartu kredit dan memberikan keyakinan bahwa model dapat efektif memberikan peringatan dini terhadap potensi tindak pidana penipuan.

Penelitian ini menggunakan dataset yang lebih besar dan teknik praproses data yang lebih mutakhir dibandingkan dengan penelitian sebelumnya. Dengan menggunakan metode validasi silang yang lebih canggih, model ini terbukti memiliki keandalan dan generalisasi yang lebih baik dalam berbagai skenario transaksi. Hasil ini sejalan dengan temuan dari penelitian-penelitian sebelumnya yang juga menggunakan algoritma *Random Forest* untuk deteksi penipuan, namun dengan peningkatan akurasi dan efektivitas yang lebih tinggi dalam penelitian ini.

Setelah penelitian ini selesai, beberapa langkah selanjutnya yang dapat diambil adalah mengimplementasikan model ini dalam sistem transaksi keuangan nyata untuk menguji kinerja dan efektivitasnya dalam lingkungan operasional. Selain itu, pengembangan model lebih lanjut dengan menggabungkan algoritma *machine learning* lain, seperti *Gradient Boosting* atau *Deep Learning*, dapat meningkatkan akurasi dan kecepatan deteksi. Aspek keamanan data dalam proses praproses dan pelatihan model juga perlu diperkuat untuk mengurangi risiko kebocoran data dan memastikan privasi pengguna. *Monitoring* dan pemeliharaan rutin terhadap model yang diterapkan akan memastikan model tetap relevan dan akurat seiring dengan perubahan pola transaksi dan teknik penipuan. Bekerja sama dengan industri keuangan dan teknologi juga menjadi langkah penting untuk mengadopsi dan menyempurnakan model ini sesuai dengan kebutuhan dan tantangan yang ada di lapangan. Dengan melakukan langkah-langkah ini, penelitian ini dapat memberikan kontribusi yang signifikan dalam upaya deteksi dan pencegahan penipuan kartu kredit, serta meningkatkan keamanan dan kepercayaan dalam sistem keuangan digital.

5. DAFTAR PUSTAKA

- Afriyie, J. K., Tawiah, K., Pels, W. A., Addai-Henne, S., Dwamena, H. A., Owired, E. O., Ayeh, S. A., & Eshun, J. (2023). A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. *Decision Analytics Journal*, 6. <https://doi.org/10.1016/j.dajour.2023.100163>
- Alhamdani, F. D. S., Dianti, A. A., & Azhar, Y. (2021). Segmentasi Pelanggan Berdasarkan Perilaku Penggunaan Kartu Kredit Menggunakan Metode K-Means Clustering. *JISKA (Jurnal Informatika Sunan Kalijaga)*, 6(2), 70–77. <https://doi.org/https://doi.org/10.14421/jiska.2021.6.2.70-77>
- Alsarhan, A., Hussein, F., Moh, S., & El-Salhi, F. S. (2021). The Effect of Preprocessing Techniques, Applied to Numeric Features, on Classification Algorithms' Performance. *Data*, 6(2). <https://doi.org/https://doi.org/10.3390/data6020011>
- Ambarwati, D. (2020). Implementasi Metode Random Forest dan Artificial Neural Network pada Imbalanced dan Balanced Data dalam Mendeteksi Penipuan Kartu Kredit [Universitas Gadjah Mada]. <http://etd.repository.ugm.ac.id/>
- Apriwandi. Herycson. (2022). Cyber Crime Dan Fraud Kartu Kredit Dan Kartu Debit: Perspektif Akuntansi. *JUEB (Jurnal Ekonomi Dan Bisnis)*, 1(3), 111–124. <https://doi.org/https://doi.org/10.57218/jueb.v1i3.277>
- Armiani, R., & Agustini, E. P. (2022). Analisa Fraud Pada Transaksi Kartu Kredit Menggunakan Algoritma Random Forest. *J-TIT (Jurnal Teknologi Informasi Dan Terapan)*, 9(2), 118–126. <https://doi.org/https://doi.org/10.25047/jtit.v9i2.297>
- Batubara, M., Ramadan, P., Zuhro, A., Hasibuan, S., Nasution, A., Syahputra, R., Aisah, S., Ekonomi, F., & Islam, B. (2022). Pengaruh Perilaku Konsumtif Masyarakat terhadap Penggunaan Kartu Kredit. *VISA (Journal of Visions and Ideas)*, 2(2), 172–180. <https://doi.org/47467/visa.v2i2.971>
- Carcillo, F., Le Borgne, Y. A., Caelen, O., Kessaci, Y., Oblé, F., & Bontempi, G. (2021). Combining unsupervised and supervised learning in credit card fraud detection. *Information Sciences*, 557, 317–331. <https://doi.org/https://doi.org/10.1016/j.ins.2019.05.042>
- Chairunisa, R., Adiwijaya, & Astuti, W. (2020). Perbandingan CART dan Random Forest untuk Deteksi Kanker berbasis Klasifikasi Data Microarray. *JURNAL RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, 4(5), 805–812. <https://doi.org/https://doi.org/10.29207/resti.v4i5.2083>
- Diana, Y., Hadi, F., Ekonomi, F., Bisnis, D., Putra Indonesia, U., Padang, Y., Lubuk, J. R., & Padang, B. (2023). Analisa Penjualan Menggunakan Algoritma K-MEDOIDS untuk Mengoptimalkan Penjualan Barang. *JOISIE (Journal Of Information System And Informatics Engineering)*, 7(1), 97–103. <https://doi.org/https://doi.org/10.35145/joisie.v7i1.2905>
- Dornadula, V. N., & Geetha, S. (2019). Credit Card Fraud Detection using Machine Learning Algorithms. *Procedia Computer Science*, 165, 631–641. <https://doi.org/10.1016/j.procs.2020.01.057>
- Fadli, M., & Saputra, R. A. (2023). Classification And Evaluation Of Performance Models Random Forest For Stroke Prediction. *JT (Jurnal Teknik)*, 12(2). <https://doi.org/http://dx.doi.org/10.31000/jt.v12i2.9099>
- Febriady, M., Samsuryadi, & Rini, D. P. (2022). Klasifikasi Transaksi Penipuan Pada Kartu Kredit Menggunakan Metode Resampling Dan Pembelajaran Mesin. *JURNAL Media Informatika Budidarma*, 6(2), 1010–1016. <https://doi.org/10.30865/mib.v6i2.3765>
- Hendarsyah, D., Tinggi, S., Ekonomi, I., & Bengkalis, S. (2020). Analisis perilaku konsumen dan keamanan kartu kredit perbankan. *Jurnal Perbankan Syariah*, 1(1), 85–96. <https://doi.org/https://doi.org/10.46367/jps.v1i1.204>
- Jain, S. (2019). A comparative analysis of various credit card fraud detection techniques. *International Journal of Recent Technology and Engineering*, 7(5), 402–407. <https://www.researchgate.net/publication/332264296>
- Kumar Manjhvar, A., & Goyal, R. (2020). Review on Credit Card Fraud Detection using Data Mining Classification Techniques & Machine Learning Algorithms. *IJRAR (International Journal of Research and Analytical Reviews)*, 7(1), 972–975. www.ijrar.org

- Kurniawan, A., & Yulianingsih, Y. (2021). Pendugaan Fraud Detection pada kartu kredit dengan Machine Learning. *KILAT (Kajian Ilmu Dan Teknologi)*, 10(2), 320–325. <https://doi.org/10.33322/kilat.v10i2.1482>
- Lestari, T. S., & Sirodj, D. A. N. (2022). Klasifikasi Penipuan Transaksi Kartu Kredit Menggunakan Metode Random Forest. *Jurnal Riset Statistika*, 1(2), 160–167. <https://doi.org/10.29313/jrs.v1i2.525>
- Megalooikonomou, K. G., & Beligiannis, G. N. (2023). Random Forests Machine Learning Applied to PEER Structural Performance Experimental Columns Database. *Applied Sciences*, 13(23), 12821. <https://doi.org/10.3390/app132312821>
- Ningsih, P. T. S., Gusvarizon, M., & Hermawan, R. (2022). Analisis Sistem Pendeteksi Penipuan Transaksi Kartu Kredit dengan Algoritma Machine Learning. *JTIK (Jurnal Teknologi Informatika Dan Komputer)*, 8(2), 386–401. <https://doi.org/10.37012/jtik.v8i2.1306>
- Pourhabibi, T., Ong, K. L., Kam, B. H., & Boo, Y. L. (2020). Fraud detection: A systematic literature review of graph-based anomaly detection approaches. *Decision Support Systems*, 133. <https://doi.org/10.1016/j.dss.2020.113303>
- Sitohang, E. H., Setiabudi, D. H., & Ananda, S. A. (2021). Penerapan Modified ADASYN untuk Meningkatkan Akurasi Pendeteksian Pola Fraud pada Transaksi Kartu Kredit. *Jurnal Infra*, 9(2), 84–90.
- Triyanto, S., Sunyoto, A., & Arief, M. R. (2021). Analisa Klasifikasi Bencana Banjir Berdasarkan Curah Hujan Menggunakan Algoritma Naive Bayes. *JOISIE (Journal Of Information System And Informatics Engineering)*, 5(2), 109–117. <https://doi.org/https://doi.org/10.35145/joisie.v5i2.1785>
- Werdiningsih, I., Purwanti, E., Wira Aditya, G. R., Hidayat, A. R., Athallah, R. S. R., Sahar, V. A., Wibisono, T. S., & Nura Somba, D. F. (2023). Identifying Credit Card Fraud in Illegal Transactions Using Random Forest and Decision Tree Algorithms. *Jurnal Sisfokom (Sistem Informasi Dan Komputer)*, 12(3), 477–484. <https://doi.org/10.32736/sisfokom.v12i3.1730>