

ANALISIS KLASIFIKASI TRANSAKSI PENIPUAN KARTU KREDIT MENGUNAKAN MODEL ALGORITMA KLASIFIKASI NAÏVE BAYES

Windy Naailah Azzahra, Muhammad Agung Nugroho,
Rizka Aisyah Alfalah, Agung Gunawan, Amrin Imron, Besus Maula Sulthon

Sistem Informasi, Universitas Bina Sarana Informatika

Jl. Kramat raya No 18 Jakarta Pusat, Indonesia

19235139@gmail.com

ABSTRAK

Perkembangan transaksi digital dan penggunaan kartu kredit yang semakin meningkat menyebabkan risiko terjadinya penipuan transaksi (*credit card fraud*) juga semakin tinggi. Aktivitas penipuan kartu kredit dapat menimbulkan kerugian finansial bagi pengguna maupun pihak perbankan sehingga diperlukan sistem deteksi yang mampu mengidentifikasi transaksi mencurigakan secara cepat dan akurat. Permasalahan yang sering terjadi adalah sulitnya membedakan transaksi normal dan transaksi penipuan karena pola data yang kompleks serta jumlah data transaksi yang sangat besar. Penelitian ini bertujuan untuk menganalisis klasifikasi transaksi penipuan kartu kredit menggunakan model algoritma Naïve Bayes guna membantu proses deteksi *fraud* secara efektif. Metode yang digunakan adalah klasifikasi data mining dengan tahapan pengumpulan dataset, *preprocessing* data, pembagian data latih dan data uji, serta pelatihan model menggunakan algoritma Naïve Bayes. Hasil penelitian menunjukkan bahwa algoritma Naïve Bayes mampu mengklasifikasikan transaksi penipuan dan transaksi normal dengan baik sehingga dapat digunakan sebagai alternatif metode deteksi dini untuk meningkatkan keamanan transaksi kartu kredit.

Kata kunci : Klasifikasi, Penipuan Kartu Kredit, Naïve Bayes, Fraud Detection, Data Mining, Transaksi Digital

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk pada sektor keuangan dan sistem pembayaran [1]. Kemajuan teknologi tersebut mendorong meningkatnya penggunaan kartu kredit sebagai salah satu alat pembayaran non-tunai yang praktis, cepat, dan efisien [2]. Salah satu metode pembayaran yang banyak digunakan masyarakat adalah kartu kredit karena dinilai efisien, fleksibel, dan dapat digunakan dalam berbagai jenis transaksi, baik secara langsung maupun melalui platform digital [3]. Peningkatan pengguna kartu kredit di era digital turut mendorong pertumbuhan transaksi elektronik yang semakin tinggi dari tahun ke tahun [4].

Dibalik kemudahan tersebut muncul berbagai ancaman kejahatan siber (*cybercrime*) yang digunakan untuk menggambarkan aktivitas kejahatan yang memanfaatkan computer atau jaringan computer sebagai alat, target, maupun tempat terjadinya tindak kejahatan [5], salah satunya adalah penipuan transaksi kartu kredit (*credit card fraud*). Penipuan kartu kredit merupakan tindakan ilegal yang dilakukan oleh pihak tertentu dengan memanfaatkan data atau identifikasi kartu kredit untuk melakukan transaksi tanpa izin pemilik kartu [6]. Aktivitas *fraud* dapat terjadi melalui berbagai cara, seperti pencurian data kartu, pemalsuan identitas, penyalahgunaan informasi transaksi, hingga serangan digital yang memanfaatkan kelemahan sistem keamanan. Kejahatan ini tidak hanya menyebabkan kerugian finansial yang besar bagi pengguna kartu kredit, pihak perbankan, dan penyedia layanan pembayaran digital, tetapi juga dapat

menurunkan tingkat kepercayaan masyarakat terhadap keamanan transaksi elektronik [7][8].

Seiring meningkatnya jumlah transaksi digital, proses identifikasi transaksi penipuan menjadi semakin kompleks. Volume data transaksi yang sangat besar serta pola aktivitas *fraud* yang terus berkembang menyebabkan transaksi penipuan sering kali memiliki karakteristik yang hampir menyerupai transaksi normal sehingga sulit dideteksi secara manual [9] kondisi tersebut menimbulkan permasalahan dalam upaya membedakan transaksi normal dan transaksi penipuan secara cepat dan akurat. Oleh karena itu, diperlukan suatu metode analisis yang mampu melakukan klasifikasi transaksi secara otomatis untuk membantu proses deteksi dini terhadap aktivitas mencurigakan.

Salah satu pendekatan yang dapat digunakan adalah Teknik data mining. Data mining merupakan proses pengumpulan serta pemanfaatan data historis untuk mengidentifikasi pola, keteraturan, maupun hubungan tertentu dalam kumpulan data yang berukuran besar [10]. Dalam bidang keamanan transaksi digital, data mining dapat dimanfaatkan untuk mendeteksi aktivitas mencurigakan berdasarkan pola transaksi yang telah terjadi sebelumnya. Salah satu algoritma klasifikasi yang sering digunakan dalam proses deteksi *fraud* adalah algoritma Naïve Bayes. Algoritma ini memiliki kemampuan melakukan perhitungan probabilitas secara sederhana, cepat, serta mampu menangani data dalam jumlah besar sehingga berpotensi menghasilkan klasifikasi yang baik pada proses deteksi *fraud* [11].

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis klasifikasi transaksi

penipuan kartu kredit menggunakan algoritma naïve bayes sebagai metode klasifikasi dalam Teknik data mining. Rencana penyelesaian masalah dilakukan melalui tahapan pengumpulan dataset transaksi kartu kredit, preprocessing data, pembagian data latih dan data uji, pembagunan model klasifikasi menggunakan aplikasi rapid miner, serta evaluasi kinerja model untuk mengetahui kemampuan algoritma dalam mendeteksi transaksi fraud dan non-fraud.[12] Hasil penelitian diharapkan dapat menjadi referensi dalam pengembangan system deteksi penipuan transaksi digital serta mendukung peningkatan keamanan data dan transaksi elektronik.

2. TINJAUAN PUSTAKA

2.1. Data mining

Data mining, yang juga dikenal sebagai Knowledge Discovery in Database (KDD), merupakan proses pengumpulan dan pemanfaatan data historis untuk mengidentifikasi pola, keteraturan, serta hubungan tertentu dalam kumoulan data yang berukuran besar [13]. Dalam bidang keamanan transaksi digital, data mining digunakan untuk membantu mendeteksi aktivitas mencurigakan berdasarkan pola transaksi yang terdapat pada data historis. Hal ini didukung oleh penelitian terdahulu yang dilakukan oleh Fazrin Meila Azzahra Sofyan, Apriade Voutama, dan Yuyun Umaidah yang menunjukkan bahwa penerapan Teknik data mining pada proses klasifikasi mampu menghasilkan informasi yang akurat dan efektif dalam mengidentifikasi pola data, sehingga dapat dimanfaatkan untuk mendukung proses deteksi serta pengambilan Keputusan secara lebih cepat dan tepat [14].

2.2. Klasifikasi

klasifikasi Adalah salah satu Teknik dalam data mining yang digunakan untuk mengelompokkan data ke dalam kategori tertentu berdasarkan atribut yang dimiliki. Konsep klasifikasi pertama kali digunakan dalam bidang biologi oleh carolus Linnaeus untuk mengelompokkan spesies berdasarkan karakteristik fisik yang dimilikinya [15]. Metode klasifikasi bekerja dengan membangun model dari data yang telah diketahui kelasnya, kemudian model tersebut digunakan untuk memprediksi kelas pada data baru [16]. Dalam penelitian ini, klasifikasi digunakan untuk membedakan transaksi normal dan transaksi penipuan kartu kredit.

2.3. Penipuan Kartu Kredit (Credit Card Fraud)

Penipuan kartu kredit atau credit fraud merupakan Tindakan penyalahgunaan kartu kredit secara ilegal untuk memperoleh keuntungan pribadi. Data pemilik kartu dapat disalahgunakan melalui berbagai cara, antara lain penggunaan alat pembaca ilegal oleh pihak yang tidak bertanggung jawab, penipuan phishing, serta serangan peretasan pada system atau jaringan Perusahaan. Semakin

meningkatnya penggunaan transaksi elektronik menyebabkan kasus penipuan kartu kredit juga meningkatkan sehingga diperlukan system keamanan yang mampu mendeteksi transaksi fraud secara cepat dan akurat.

2.4. Algoritma Naïve Bayes

Naive bayes merupakan metode klasifikasi yang memanfaatkan atribut data untuk menghasilkan informasi dengan menggunakan pendekatan statistic dan teori probabilitas.[17] Algoritma ini bekerja dengan menghitung kemungkinan suatu data termasuk ke dalam kelas tertentu berdasarkan atribut yang dimiliki. Naïve bayes memiliki asumsi bahwa setiap atribut bersifat independent terhadap atribut lainnya.

Rumus dasar algoritma Naïve Bayes Adalah :

$$P(H|X) = \frac{P(X|H).P(H)}{P(X)} \quad (1)$$

Keterangan :

$P(H|X)$ = Probabilitas hipotesis H berdasarkan kondisi X

$P(X|H)$ = Probabilitas munculnya X berdasarkan hipotesis H

$P(H)$ = Probabilitas hipotesis H

$P(X)$ = Probabilitas munculnya X

Dalam penelitian ini :

- H merupakan kelas transaksi, yaitu fraud atau non-fraud.
- X merupakan atribut transaksi kartu kredit yang digunakan dalam proses klasifikasi.

Algoritma naïve bayes memiliki beberapa keunggulan, salah satunya Adalah kemampuannya dalam melakukan estimasi parameter yang dibutuhkan untuk proses klasifikasi berdasarkan data (training data) yang tersedia.[18] Oleh karena itu, algoritma ini banyak digunakan dalam penelitian klasifikasi data, termasuk deteksi penipuan transaksi kartu kredit.

2.5. Cybercrime

menurut Gregory Cybercrime merupakan bentuk kejahatan yang memanfaatkan computer dan jaringan internet sebagai alat maupun sasaran tindak criminal [19] Cybercrime mencakup berbagai aktivitas illegal seperti pencurian data, penipuan online, malware, dan carding. Dalam transaksi kartu kreit, cybercrime sering terjadi melalui pencurian informasi pengguna yang kemudian digunakan untuk melakukan transaksi tanpa izin pemilik asli kartu.

2.6. Rapid Miner

Rapid miner merupakan platform analisis data yang mendukung penerapan machine learning, deep learning, text mining dan predictive analytics dalam satu lingkungan kerja yang terintegrasi. RapidMiner menyediakan berbagai operator yang memudahkan pengguna dalam melakukan analisis data tanpa memerlukan pemrograman yang kompleks. Dalam penelitian ini, rapid miner digunakan untuk melakukan preprocessing data, penerapan algoritma naïve bayes,

serta evaluasi hasil klasifikasi transaksi penipuan kartu kredit.

3. METODE PENELITIAN

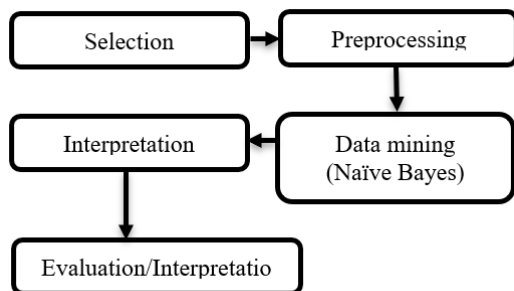
3.1. Metode Penelitian

Penelitian ini menggunakan metode kuantitatif dengan pendekatan data mining. Karena berfokus pada pengolahan data numerik untuk menemukan pola dan hubungan dalam data transaksi kartu kredit. Pola tersebut kemudian dimanfaatkan untuk mengklasifikasikan transaksi ke dalam kategori fraud (penipuan) dan non-fraud (normal, sehingga dapat mendukung proses deteksi penipuan secara lebih akurat.[20]

Metode klasifikasi yang digunakan dalam penelitian ini Adalah algoritma naïve bayes. Algoritma ini dipilih karna memiliki proses perhitungan yang sederhana, mampu menangani dataset dalam jumlah besar, serta memiliki kemampuan klasifikasi yang cukup baik dalam berbagai penelitian terkait deteksi fraud.

3.2. KDD (Knowledge Discovery in Database)

Data mining merupakan salah satu tahapan dalam proses Knowledge Discovery in Database (KDD) yang berfungsi untuk mengekstraksi pola atau model dari data menggunakan algoritma tertentu.[21] Dalam penelitian ini, data yang digunakan berupa dataset transaksi kartu kredit yang diperoleh dari sumber data public, yang terdiri atas transaksi normal (non-fraud) dan transaksi penipuan (fraud) beserta sejumlah atribut yang digunakan sebagai variable dalam proses klasifikasi menggunakan algoritma Naïve Bayes.



Gambar 1. Tahap KDD (Knowledge Discovery in Database)

- Selection : Memilih dataset Credit Card Fraud Detection dari Kaggle.
- Preprocessing : Membersihkan dan memeriksa kualitas data
- Transformation : Menentukan atribut dan label kelas (fraud/non-fraud)
- Data Mining : Menerapkan algoritma Naïve Bayes dan RapidMiner
- Evaluation : mengukur hasil menggunakan confusion matrix, accuracy, precision, dan recall.

4. HASIL DAN PEMBAHASAN

4.1. Proses Pengumpulan Data

Prosess pengumpulan data dilakukan dengan memperoleh dataset transaksi kartu kredit dari sumber data public yang sering digunakan dalam penelitian deteksi fraud. Dataset yang digunakan berasal dari Credit Card Fraud Detection Dataset yang tersedia dalam platform Kaggle. Dataset tersebut berisi 284.807 data transaksi kartu kredit dengan atribut, yang terdiri dari 284.315 transaksi non-fraud dan 492 transaksi fraud. Data ini banyak digunakan sebagai benchmark dalam penelitian deteksi penipuan kartu kredit.

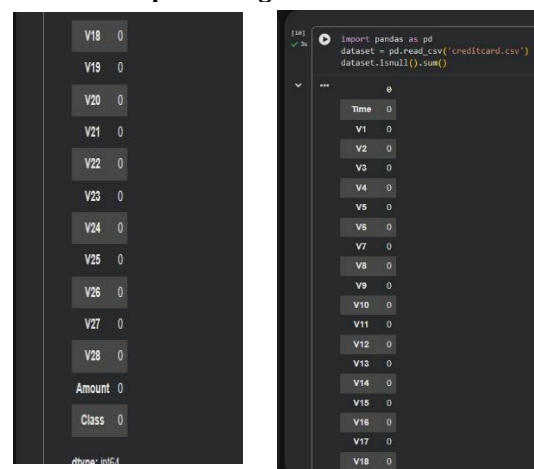
Data yang telah diperoleh kemudian diperiksa untuk memastikan kelengkapan dan kesesuaiannya dengan kebutuhan penelitian. Selanjutnya, dataset diimpor ke dalam aplikasi rapid miner untuk dilakukan proses preprocessing, pemilihan atribut, pembentukan model klasifikasi menggunakan algoritma naïve bayes, serta evaluasi hasil klasifikasi. Data yang terkumpul menjadi dasar proses analisis untuk mengidentifikasi pola transaksi dan mendeteksi kemungkinan terjadinya penipuan kartu kredit.

Dataset yang digunakan dapat diakses melalui link ini : <https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud>

4.2. Data Selection

Pada tahap data selection, dilakukan pemilihan atribut yang relevan dari dataset Credit Card Fraud Detection untuk digunakan dalam proses klasifikasi. Atribut yang dipilih meliputi variable transaksi yang terdapat dalam dataset, sedangkan atribut yang tidak berpengaruh terhadap proses analisis dapat diabaikan. Tahap ini bertujuan untuk memastikan bahwa data yang digunakan sesuai dengan kebutuhan penelitian serta dapat meningkatkan efektivitas model naïve bayes dalam mengklasifikasikan transaksi fraud dan non fraud.

4.3. Data Preprocessing



Gambar 2. Cek value

Tahap ini dilakukan pembersihan dan persiapan data sebelum proses klasifikasi. Kegiatan yang dilakukan meliputi pemeriksaan data yang hilang (missing value), penghapusan data duplikat, serta penyesuaian format data agar sesuai dengan kebutuhan analisis. Tahap ini bertujuan untuk meningkatkan kualitas data sehingga proses klasifikasi menggunakan algoritma Naïve Bayes dapat menghasilkan kinerja yang lebih optimal.

4.4. Data Transformation

Pada tahap ini data yang telah melalui proses preprocessing diubah kedalam format yang sesuai untuk proses klasifikasi menggunakan algoritma Naïve Bayes. Transformasi dilakukan dengan menyesuaikan struktur data, menentukan atribut yang digunakan, serta menetapkan atribut kelas (label) sebagai target klasifikasi, yaitu fraud dan non-fraud. Tahap ini bertujuan agar data dapat diproses secara optimal pada tahap data mining.

	◀	V24 real	◀	V25 real	◀	V26 real	◀	V27 real	◀	V28 real	◀	Amount real	◀	Class discretal	◀
1	0	0.067	0.129	-0.189	0.134	-0.021	149.520	0							
2	1	-0.340	0.167	0.126	-0.009	0.015	2.690	0							
3	3	-0.689	-0.328	-0.139	-0.355	-0.090	378.600	0							
4	0	-1.176	0.647	-0.222	0.063	0.061	121.600	0							
5	7	0.141	-0.206	0.032	0.219	0.215	69.990	0							
6	6	-0.371	-0.233	0.136	0.254	0.081	3.679	0							
7	4	-0.780	0.750	-0.287	0.035	0.005	4.990	0							
8	3	-0.850	-0.415	-0.052	-1.297	-1.085	40.800	0							
9	4	1.012	0.373	-0.384	0.012	0.142	93.200	0							
10	1	-0.385	-0.070	0.094	0.245	0.083	3.680	0							
11	3	0.501	0.251	-0.129	0.043	0.019	7.800	0							
12	3	0.997	-0.707	-0.492	0.042	-0.054	9.990	0							
13	3	0.393	0.151	-0.355	0.025	0.042	121.500	0							
14	1	0.105	0.548	0.104	0.021	0.021	27.500	0							
15	1	0.026	-0.253	-0.226	-0.185	-0.039	59.800	0							
16	7	-0.065	-0.009	-0.087	-0.181	0.129	15.990	0							
17	1	0.104	0.354	-0.382	0.083	0.037	12.990	0							

Gambar 3. Transformation dataset

4.5. Algoritma C4.5

Pada tahap data mining, algoritma C4.5 digunakan untuk membangun model klasifikasi yang dapat mengelompokkan transaksi ke dalam kategori fraud dan non-fraud berdasarkan atribut yang terdapat pada dataset.

	true 0	true 1	class precision
pred. 0	222533	68	99.97%
pred. 1	4919	326	6.22%
class recall	97.84%	82.74%	

Gambar 5 : Hasil Nilai Accuary,Recall, Precision

4.9. Hasil Recall

Hasil ini menunjukkan kemampuan model dalam menemukan seluruh data pada kelas yang dipilih.

Recall Non-Fraud(Class 0)

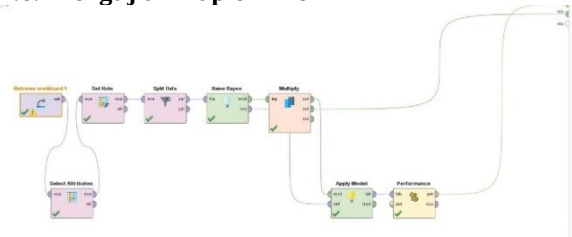
Nilai pada table :

97,84%

Artinya :

Dari seluruh transaksi normal yang ada, model berhasil mengenali 97,84% sebagai transaksi normal.

4.6. Pengujian RapidMiner



Gambar 4. Pengujian dataset pada RapidMiner

4.7. Confusion Matrix

Tabel 1. Confusion Matrix

Prediksi	True 0(non-fraud)	True1 (fraud)
Pred.0	222.533	68
Pred.1	4.919	326

Sehingga:

- True Negative (TN) = 222.5333
- False Positive (FP) = 4.919
- False Negative (FN) = 68
- True Positive (TP) = 326

4.8. Hasil Accuracy

Accuary menunjukan Tingkat ketepatan model dalam mengklasifikasi seluruh data.

Rumus :

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \times 100\%$$

$$= (326 + 222.533) / (326 + 222.533 + 4.919 + 68)$$

$$= 222.859 / 227.846$$

$$= 97,81\%$$

Nilai accuracy sebesar 97,81% menunjukan bahwa model Naïve Bayes mampu mengklasifikasikan 97,81% transaksi dengan benar. Dari seluruh data yang diuji hanya sekitar 2,19% saja yang mengalami kesalahan klasifikasi.

Recall Fraud (Class 1)

Nilai pada tabel : 82,74%

$$Rumus: Recall = \frac{TP}{TP + FN} \times 100\%$$

Perhitungan :

$$= 326 / (326 + 68)$$

$$= 326 / 394$$

$$= 82,74\%$$

Nilai recall fraud sebesar 82,74% menunjukkan bahwa model berhasil mendeteksi sekitar 83 dari setiap 100 transaksi penipuan. Hanya 68 transaksi fraud yang gagal terdeteksi dan dianggap sebagai transaksi normal

Dalam penelitian fraud detection, recall fraud merupakan indikator yang sangat penting karena menunjukkan kemampuan system dalam menemukan transaksi penipuan.

4.10. Hasil Precision

Hasil ini menunjukkan Tingkat ketepatan prediksi model.

Precision Non-Fraud (Class 0)

Nilai pada tabel:

99,97%

Artinya:

Hampir seluruh transaksi yang diprediksi sebagai non-fraud memang benar-bener transaksi normal.

Precision fraud (Class1)

Nilai pada tabel : 6,22%

Rumus:

$$Precision = \frac{TP}{TP + FP} \times 100\%$$

Perhitungan :

$$= 326 / (326 + 4.919)$$

$$= 326 / 5.245$$

$$= 6,22\%$$

Nilai precision fraud sebesar 6,22% menunjukkan bahwa dari seluruh transaksi yang diprediksi sebagai fraud, hanya 6,22% yang benar – benar fraud. Sisanya merupakan transaksi normal yang salah diklasifikasikan sebagai fraud (false positive).

Hal ini terjadi karena dataset sangat tidak seimbang, yaitu:

- Non-Fraud = 99,8%
- Fraud = 0,2%

Akibatnya model cenderung menghasilkan cukup banyak false positive.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian yang telah dilakukan, algoritma naïve bayes mampu digunakan untuk mengklasifikasikan transaksi kartu kredit ke dalam kategori fraud (penipuan) dan non-fraud (normal). Hasil pengujian menggunakan rapid miner menunjukkan nilai accuracy sebesar 97,81% yang menandakan bahwa model memiliki Tingkat ketepatan yang tinggi dalam melakukan klasifikasi. Selain itu, nilai recall fraud sebesar 82,74% menunjukkan bahwa model mampu mendeteksi Sebagian besar transaksi penipuan yang terdapat pada dataset. Meskipun nilai precision fraud masih relative rendah, secara keseluruhan algoritma naïve bayes terbukti cukup efektif dalam mendukung proses deteksi penipuan kartu kredit dan dapat dimanfaatkan sebagai salah satu metode untuk meningkatkan keamanan transaksi elektronik.

Penelitian selanjutnya disarankan untuk menerapkan Teknik penanganan data tidak seimbang (imbalanced data) seperti SMOTE atau undersampling guna meningkatkan kemampuan model dalam mendeteksi transaksi fraud. Selain itu, perlu dilakukan perbandingan dengan algoritma klasifikasi lainnya, seperti decision tree, random forest, atau support vector machine (SVM), untuk memperoleh model dengan performa yang lebih optimal. Penggunaan dataset yang lebih beragam serta pengembangan system deteksi penipuan secara real-time juga dapat menjadi alternatif untuk meningkatkan akurasi dan efektivitas system dalam mengidentifikasi transaksi penipuan kartu kredit

DAFTAR PUSTAKA

- [1] R. Sulaehani, I. Colanus, R. Drajana, and Betrisandi, "Klasifikasi Nasabah Dalam Pengelolaan Resiko Kredit Menggunakan Metode Naïve Bayes," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 6, no. 6, pp. 804–808, 2023.
- [2] T. Ramadani, C. Delopinli, R. Septiawan, and E. Ismanto, "Analisis Performa Algoritma Machine Learning dalam Mendeteksi Fraud pada Dataset Aplikasi Kartu Kredit," *J. fasilkom*, vol. 15, no. 2, pp. 383–390, 2025.
- [3] P. Putri, A. P. Wicaksono, S. Widjaja, M. F. Nugroho, and Christina, "Analisa Nilai K terhadap Pengelompokan Penjualan Tiket pada K-Means dengan Metode Elbow dan Silhouette Elbow and Silhouette Methods for K Value Analysis of Ticket Sales Grouping," *Sist. J. Sist. Inf.*, vol. 13, no. 1, pp. 28–38, 2024.
- [4] L. Oriana, A. Dwi, S. Wati, A. P. Ramahdani, N. N. Safira, and E. Ismanto, "Peningkatan Kinerja Model Random Forest untuk Deteksi Kecurangan Kartu Kredit Menggunakan RandomizedSearchCV," *J. FASILKOM*, vol. 15, no. 2, pp. 229–237, 2025.
- [5] A. Alhakim and Sofia, "KAJIAN NORMATIF PENANGANAN CYBER CRIME DI SEKTOR PERBANKAN DI INDONESIA," *e-Journal Komunitas Yust. Univ. Pendidik. Ganesha*, vol. 4, no. 2, pp. 377–385, 2021.
- [6] S. Sintia, A. Khautsar, D. Puspitasari, and P. Mustika, "Algoritma Naïve Bayes Untuk Memprediksi Kredit Macet Pada Koperasi Simpan Pinjam," *J. Inform. UPGRIS*, vol. 4, no. 2, p. 1, 2018.
- [7] J. Manajemen *et al.*, "Implementasi Algoritma Random Forest Dalam Klasifikasi Risiko Gagal Bayar Kartu Kredit Pada Nasabah Bank," *J. Manaj. Teknol. dan Sist. Inf.*, vol. 5, no. 1, pp. 1050–1059, 2025.
- [8] F. D. Prasetya, I. A. Kautsar, U. Indahyanti, and S. Busono, "RANCANG BANGUN SISTEM INFORMASI LAYANAN ADMINISTRASI DESA BERBASIS WEB (STUDI KASUS: DESA GERBO PASURUAN)," *J. Mhs. Tek. Inform.*, vol. 10, no. 3, pp. 3651–3658, 2026.

- [9] M. Agustriya and M. Ula, "Analisis Kinerja Algoritma Klasifikasi Naïve Bayes Menggunakan Genetic algorithm dan Bagging untuk Data Publik Risiko Transaksi Kartu Kredit Performance Analysis of Naïve bayes Classification Algorithm Using Genetic algorithm and Bagging for Public Data o," *J. Sist. dan Teknol. Inf.*, vol. 12, no. 3, p. 8, 2024, doi: 10.26418/justin.v12i3.80136.
- [10] L. Swastina, "Penerapan Algoritma C4 . 5 Untuk Penentuan Jurusan Mahasiswa," *J. GEMA Aktual.*, vol. 2, no. 1, p. 6, 2013.
- [11] M. S. Novita, "IMPLEMENTASI PEMBERIAN SANKSI TERHADAP TINDAK PIDANA PEMALSUAN DATA DITINJAU MENURUT UNDANG-UNDANG NO. 11 TAHUN 2008 TENTANG INFORMASI TRANSAKSI ELEKTRONIK," *STIH Painan*, vol. 10, no. 11, pp. 123–134, 2023.
- [12] L. Nurzahra, M. S. Nidhom, C. Adipradana, and A. N. Izzati, "ANALISIS PENENTUAN KREDIT NASABAH PADA BUMDES MENGGUNAKAN ALGORITMA NAIVE BAYES (STUDI KASUS: BUMDES BARIKLANA DESA SIDOWAREK KECAMATAN PLEMAHAN KABUPATEN KEDIRI)," *J. Compos. Soc. humanisme*, vol. 1, no. 3, pp. 35–48, 2024.
- [13] M. Badrul, "Algoritma asosiasi dengan algoritma apriori untuk analisa data penjualan," *J. Pilar Nusa Mandiri*, vol. XII, no. 2, pp. 121–129, 2016.
- [14] F. M. A. Sofyan, A. Voutama, and Y. Umaidah, "Penerapan algoritma c4.5 untuk prediksi penyakit paru-paru menggunakan rapidminer," *J. Mhs. Inform.*, vol. 7, no. 2, pp. 1409–1415, 2023.
- [15] Y. Mardi, "Data Mining : Klasifikasi Menggunakan Algoritma C4.5," *J. Edik Inform. Penelit. Bid. Komput. Sains dan Pendidik. Inform.*, vol. 2, no. 1, p. 7, 2019.
- [16] A. H. Nasrullah, "IMPLEMENTASI ALGORITMA DECISION TREE UNTUK KLASIFIKASI PRODUK LARIS," *J. Ilm. Ilmu Komput.*, vol. 7, no. 2, pp. 45–51, 2021.
- [17] S. Reny Wijayanti¹, "ANALISA KLASIFIKASI KARTU KREDIT MENGGUNAKAN ALGORITMA NAIVE BAYES," *Pros. SINTAK*, vol. 1, no. 1, pp. 443–447, 2018.
- [18] A. Susilo, "Perbandingan Kinerja K-Nearest Neighbors dan Naive Bayes Untuk Klasifikasi Perilaku Nasabah Pada Pembayaran Kredit Bank," *J. J. Sains Dan Teknol.*, vol. 3, no. 3, pp. 364–379, 2023.
- [19] D. A. Arifah, "KASUS CYBERCRIME DI INDONESIA Indonesia's Cybercrime Case," *J. Bisnis dan Ekon.*, vol. 18, no. 2, pp. 185–195, 2011.
- [20] R. Apriani, "PERLINDUNGAN HUKUM BAGI NASABAH PEMEGANG KARTU KREDIT ATAS PEMALSUAN DATA YANG DILAKUKAN OLEH PIHAK MARKETING KARTU KREDIT," *LamLaj*, vol. 4, no. 1, pp. 119–128, 2019.
- [21] M. A. Sembiring, M. Fitri, L. Sibuea, and A. Sapta, "Analisa kinerja algoritma c.45 dalam memprediksi hasil belajar," *J. Sci. Soc. Res.*, vol. 4307, no. February, pp. 73–79, 2018.