JURNAL FASILKOM
Volume 15 No. 2 | Agustus 2025: 383-390

P-ISSN : 2089-3353
E-ISSN : 2808-9162

Analisis Performa Algoritma *Machine Learning* dalam Mendeteksi *Fraud* pada Dataset Aplikasi Kartu Kredit

Tasya Ramadani[1], Crystian Delopinli[2], Raffi Septiawan[3], Edi Ismanto[4]
[1,2,3,4]Teknik Informatika, Ilmu Komputer, Universitas Muhammadiyah Riau
[1]230401318@student.umri.ac.id*, [2]230401338@student.umri.ac.id, [3]230401155@student.umri.ac.id,
[4]edi.ismanto@umri.ac.id

Abstract

The increasing number of credit card fraud cases, coupled with the rapid development of digital financial transactions, demands a more precise and reliable detection system. This study aims to compare the performance of three machine learning algorithms, namely Random Forest, logistic regresi and SVM, in detecting fraud in a credit card application dataset. The research data is sourced from real credit card transaction records over a period of one year. The methodology used includes building a classification model to identify fraudulent transactions and implementing a two-period model to explore the interactions between consumers, merchants, and card issuers. The analysis results show that the Random Forests algorithm provides optimal performance with superior accuracy and detection rates compared to the SVM and logistic regresi. Furthermore, a structural study shows that merchant profit margins and low funding costs contribute to maintaining the balance of the credit card system. Other findings emphasize the characteristics of credit cards as network goods, where the more merchants accept credit cards, the higher their adoption by consumers. The use of appropriate machine learning algorithms, supported by appropriate policies, can improve the effectiveness of fraud detection while strengthening the stability of the digital financial ecosystem.

Keywords: *Fraud, machine learning algorithms, fraud detection, random forests, and credit cards*

Abstrak

Meningkatnya kasus penipuan kartu kredit seiring pesatnya perkembangan transaksi keuangan digital menuntut adanya sistem deteksi yang lebih tepat dan andal. Penelitian ini bertujuan untuk membandingkan kinerja tiga algoritma machine learning, yaitu Random Forest, Logistic regresi, dan SVM dalam mendeteksi tindak kecurangan pada dataset aplikasi kartu kredit. Data penelitian bersumber dari catatan transaksi kartu kredit nyata selama satu tahun. Metodologi yang digunakan mencakup pembangunan model klasifikasi untuk mengenali transaksi curang serta penerapan model dua-periode guna mengeksplorasi interaksi antara konsumen, pedagang, dan penerbit kartu. Hasil analisis menunjukkan bahwa algoritma Random Forests memberikan performa paling optimal dengan akurasi dan tingkat deteksi yang lebih unggul dibandingkan SVM dan logistitic regresi. Selain itu, studi struktural memperlihatkan bahwa faktor margin keuntungan pedagang dan rendahnya biaya dana berkontribusi dalam menjaga keseimbangan sistem kartu kredit. Temuan lainnya menegaskan karakteristik kartu kredit sebagai barang jaringan (network goods), di mana semakin banyak pedagang yang menerima kartu kredit, semakin tinggi pula adopsinya oleh konsumen. Pemanfaatan algoritma machine learning yang sesuai, didukung oleh kebijakan yang tepat, dapat meningkatkan efektivitas deteksi penipuan sekaligus memperkuat stabilitas ekosistem keuangan digital.

Kata kunci: kecurangan, algoritma *machine learning*, deteksi penipuan, random forest, dan kartu kredit.

1. Pendahuluan

Perkembangan teknologi informasi telah mendorong peningkatan signifikan dalam penggunaan kartu kredit sebagai alat pembayaran non-tunai. Namun, seiring dengan peningkatan volume transaksi, risiko terhadap penipuan kartu kredit juga meningkat secara drastis. Berdasarkan laporan tahunan dari CyberSource, meskipun persentase kerugian akibat penipuan online tetap stabil pada kisaran 1,4% dari total pembayaran daring selama periode 2006–2008, nilai absolut kerugian terus meningkat seiring dengan bertumbuhnya transaksi e-commerce. Pada tahun 2008, total kerugian akibat penipuan online diperkirakan mencapai USD 4 miliar, meningkat sebesar 11% dibandingkan tahun sebelumnya yang mencapai USD 3,6 miliar [1].

Penipuan kartu kredit tidak hanya menimbulkan kerugian ekonomi, tetapi juga berkontribusi terhadap pembiayaan kejahatan terorganisir, perdagangan narkotika internasional, dan pendanaan aktivitas terorisme. Selain itu, survei menunjukkan bahwa sekitar 70% konsumen di Amerika Serikat menyatakan kekhawatiran serius terhadap risiko pencurian identitas sebagai dampak dari penipuan ini.Oeh karena itu, deteksi dini terhadap aktivitas penipuan menjadi prioritas utama bagi lembaga

P-ISSN : 2089-3353
E-ISSN : 2808-9162

keuangan guna meminimalisasi risiko dan meningkatkan keamanan sistem pembayaran. Penipuan kartu kredit pada dasarnya terbagi menjadi dua jenis: penipuan aplikasi dan penipuan perilaku [1-2].

Penipuan aplikasi terjadi ketika pelaku kejahatan memperoleh kartu baru dari perusahaan penerbit dengan menggunakan informasi palsu atau informasi milik orang lain. Penipuan perilaku dapat dibagi menjadi empat jenis: pencurian surat, kartu dicuri/hilang, kartu palsu, dan penipuan "pemegang kartu tidak hadir". Penipuan pencurian surat terjadi ketika pelaku mencegat kartu kredit yang dikirim lewat pos sebelum sampai ke tangan pemilik kartu, atau mencuri informasi pribadi dari laporan bank dan kartu kredit [3].

Penipuan kartu dicuri atau hilang terjadi ketika pelaku mendapatkan kartu kredit melalui pencurian dompet/tas atau menemukan kartu yang hilang dan menggunakannya. Namun, dengan meningkatnya penggunaan transaksi online, terdapat peningkatan signifikan dalam penipuan kartu palsu dan penipuan "pemegang kartu tidak hadir". Pada kedua jenis penipuan ini, informasi kartu kredit diperoleh tanpa sepengetahuan pemilik kartu, lalu digunakan untuk membuat kartu palsu atau untuk melakukan transaksi "pemegang kartu tidak hadir", yaitu melalui surat, telepon, atau internet [4].

Informasi pemilik kartu bisa didapatkan melalui berbagai cara, seperti karyawan yang mencuri informasi menggunakan alat pembaca ilegal (swipers), penipuan phishing, atau melalui peretasan jaringan komputer perusahaan. Dalam kasus penipuan "pemegang kartu tidak hadir", detail kartu kredit digunakan dari jarak jauh untuk melakukan transaksi penipuan. Metode deteksi penipuan umumnya diklasifikasikan menjadi dua pendekatan utama, yaitu supervised dan unsupervised learning. pada pendekatan supervised, model prediktif dibangun berdasarkan data historis yang telah dilabeli, yakni transaksi yang telah diklasifikasikan sebagai penipuan (fraudulent) dan bukan penipuan (legitimate). Model tersebut kemudian digunakan untuk mengklasifikasikan transaksi baru. Sebaliknya, pada pendekatan unsupervised, deteksi dilakukan dengan mengidentifikasi transaksi yang menyimpang dari pola umum sebagai potensi penipuan [5-6].

Meskipun berbagai teknik data mining telah diterapkan secara luas dalam sistem deteksi penipuan, jumlah studi yang secara khusus mengevaluasi kinerja metode-metode tersebut dalam konteks penipuan kartu kredit masih terbatas. Penelitian terdahulu banyak berfokus pada penggunaan neural networks, sementara teknik lain seperti case-based reasoning dan hidden Markov *models* juga telah dilaporkan. Studi terbaru mengevaluasi performa beberapa algoritma, termasuk SVM dan random forests, dan menemukan bahwa metode ensemble seperti random forests memiliki kinerja yang sangat kompetitif, khususnya ketika digunakan dengan pendekatan agregasi data transaksi dalam rentang waktu tertentu.

Dalam studi ini, peneliti mengevaluasi dan membandingkan tiga pendekatan populer dalam deteksi penipuan kartu kredit, yaitu SVM, *logistic regresi* dan *random forests*. Pemilihan ketiga metode ini didasarkan pada kombinasi antara kemudahan implementasi, ketersediaan secara luas dalam perangkat lunak statistik, serta efektivitas yang telah terbukti dalam literature. SVM merupakan teknik pembelajaran statistik dengan dasar teoritis yang kuat dan kapabilitas generalisasi yang tinggi [7].

Berbeda dengan *neural networks* yang rentan terhadap overfitting dan kesalahan lokal (*local minima*), SVM memiliki kemampuan menghasilkan solusi global melalui pendekatan optimisasi yang disertai pemilihan model internal. Sementara itu, *random forests* merupakan metode *ensemble* berbasis pohon keputusan yang menggabungkan teknik bagging dan random subspace, yang memungkinkan pembentukan banyak pohon keputusan secara acak untuk menghasilkan prediksi yang stabil dan akurat. Metode ini dikenal efisien secara komputasi, robust terhadap noise, dan memiliki hanya dua parameter utama yang perlu ditentukan. Studi sebelumnya menunjukkan bahwa random forests sering kali menunjukkan performa yang unggul dibandingkan metode lain, termasuk SVM dan l*ogistic regression* [8].

Dengan menggunakan dataset transaksi nyata dari sistem kartu kredit internasional, penelitian ini bertujuan untuk: (1) menganalisis performa ketiga algoritma dalam mendeteksi transaksi penipuan, dan (2) memberikan rekomendasi terkait implementasi model deteksi yang efisien, akurat, dan praktis untuk digunakan oleh institusi keuangan. Penipuan kartu kredit pada dasarnya terbagi menjadi dua jenis: penipuan aplikasi dan penipuan perilaku . Penipuan aplikasi terjadi ketika pelaku kejahatan memperoleh kartu baru dari perusahaan penerbit dengan menggunakan informasi palsu atau informasi milik orang lain. Penipuan perilaku dapat dibagi menjadi empat jenis: pencurian surat, kartu dicuri/hilang, kartu palsu, dan penipuan "pemegang kartu tidak hadir". Penipuan pencurian surat terjadi ketika pelaku mencegat kartu kredit yang dikirim lewat pos sebelum sampai ke tangan pemilik kartu, atau mencuri informasi pribadi dari laporan bank dan kartu kredit [9,10].

Penipuan kartu dicuri atau hilang terjadi ketika pelaku mendapatkan kartu kredit melalui pencurian dompet/tas atau menemukan kartu yang hilang dan

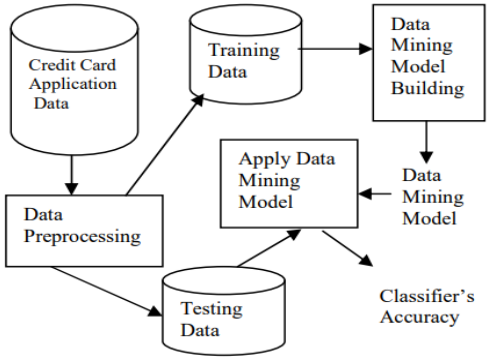
P-ISSN : 2089-3353
E-ISSN : 2808-9162

menggunakannya. Namun, dengan meningkatnya penggunaan transaksi online, terdapat peningkatan signifikan dalam penipuan kartu palsu dan penipuan "pemegang kartu tidak hadir". Pada kedua jenis penipuan ini, informasi kartu kredit diperoleh tanpa sepengetahuan pemilik kartu, lalu digunakan untuk membuat kartu palsu atau untuk melakukan transaksi "pemegang kartu tidak hadir", yaitu melalui surat, telepon, atau internet [11].

Informasi pemilik kartu bisa didapatkan melalui berbagai cara, seperti karyawan yang mencuri informasi menggunakan alat pembaca ilegal (swipers), penipuan *phishing*, atau melalui peretasan jaringan komputer perusahaan. Dalam kasus penipuan "pemegang kartu tidak hadir", detail kartu kredit digunakan dari jarak jauh untuk melakukan transaksi penipuan.

2. Metode Penelitian

Penelitian ini menerapkan metode *data mining* dalam upaya mendeteksi indikasi penipuan pada aplikasi kartu kredit. Data yang digunakan berasal dari *Credit Card Application Data* yang terlebih dahulu melalui tahap pra-pemrosesan, mencakup pembersihan dari *missing values*, duplikasi, serta *outliers*, kemudian dilakukan normalisasi dan pemilihan fitur penting. Selanjutnya, dataset dibagi menjadi dua bagian, yaitu *training data* untuk proses pelatihan algoritma dan *testing data* untuk mengevaluasi performa model.



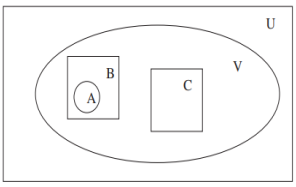
Gambar 1. Model Yang Diusulkan

Gambar 1 tahap awal dimulai dari Pengumpulan Data set data yang digunakan berupa Credit Card Application Data yang memuat atribut calon pemegang kartu. Lalu pada tahap pra-pemrosesan data, data dibersihkan dari *missing values,* duplikasi, dan outliers, kemudian dilakukan normalisasi serta pemilihan fitur penting agar siap digunakan. Dataset dipisahkan menjadi training data untuk melatih algoritma dan testing data untuk menguji performa model.Pembangunan Model Algoritma *Support Vector Machines* (SVM), Random Forests dan Regresi Logistik digunakan untuk membangun model deteksi fraud.Penerapan Model diterapkan pada testing data untuk mengklasifikasikan aplikasi kartu kredit sebagai normal atau fraud. Evaluasi Model kinerja model dievaluasi menggunakan akurasi, presisi, *recall* dan *F1-score* untuk menentukan algoritma terbaik.

2.1 Dataset

Dataset ini mencakup data selama 13 bulan, dari Januari 2006 hingga Januari 2007, dengan sekitar 50 juta (49.858.600 transaksi) transaksi kartu kredit yang dilakukan oleh sekitar satu juta (1.167.757 kartu kredit) kartu kredit dari satu negara. Untuk keperluan penelitian ini, kami menyebut dataset seluruh transaksi tersebut sebagai dataset U (Gambar 2). Sebuah subset yang jauh lebih kecil dari dataset besar ini disebut dataset A, yang berisi 2.420 transaksi penipuan yang diketahui, yang berasal dari 506 kartu kredit [7].

Salah satu atribut kategorikal, yaitu jenis transaksi, memberi label pada transaksi berdasarkan jenisnya, seperti pembelian ritel, *cash advance*, transfer, dan sebagainya. Karena diduga bahwa penipuan lebih sering terjadi hanya pada beberapa jenis transaksi tertentu, kami membandingkan jenis-jenis transaksi dalam dataset A (yang berisi transaksi penipuan yang teramati) dengan jenis transaksi dalam dataset U (yang merupakan dataset lengkap). Kami menemukan bahwa hampir 95% dari transaksi penipuan yang teramati (dalam dataset A) merupakan pembelian ritel, dibandingkan dengan kurang dari 49% pada dataset U.
Dibandingkan dengan dataset U, transaksi penipuan yang teramati hanya termasuk dalam beberapa kategori saja: transaksi ritel**,** pembayaran non-terarah transaksi ritel**,** pembayaran non-terarah**,** dan item cek. Oleh karena itu, kami mempartisi dataset U agar hanya mencakup jenis transaksi yang terdapat dalam dataset penipuan (A). Dataset U yang telah dikurangi ini terdiri dari 31.671.185 transaksi**,** dan kami menyebut dataset hasil reduksi ini sebagai dataset V [12].



Dataset U: All transactions	49,858,600 transactions
Dataset A: Fraud Dataset	2,420 transactions
Dataset B: All transactions with Fraudulent Credit Cards	37,280 transactions
Dataset V:All transactions with transaction types where *fraud* occurred	31,671,185 transactions
Dataset C: Random sample of transactions from dataset V-B	340,589 transactions

Gambar 2. Deskripsi Kumpulan Data

Gambar 2 untuk membandingkan prediksi penipuan kartu kredit menggunakan berbagai teknik, kami memerlukan sekumpulan transaksi yang terdiri dari transaksi penipuan yang sudah diketahui dan transaksi legal yang teramati atau tidak terdeteksi. Dataset A berisi kasus transaksi penipuan yang sudah

P-ISSN : 2089-3353
E-ISSN : 2808-9162

diketahui, namun kami juga memerlukan kumpulan transaksi legal yang sebanding. Kami memutuskan untuk membuat sampel acak transaksi legal dari dataset V**,** dengan mengeluarkan semua transaksi yang melibatkan 506 kartu kredit yang diketahui terlibat dalam penipuan [13].

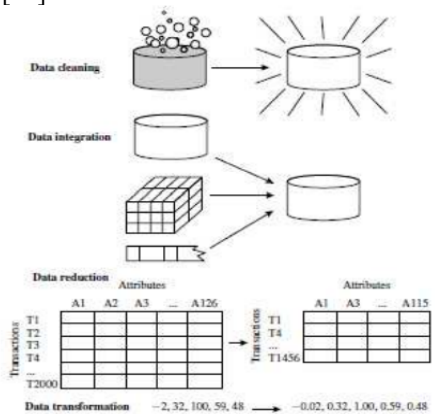
Dalam penelitian ini, kami menggunakan pendekatan serupa dan membuat atribut turunan dari atribut utama yang telah dibahas pada bagian sebelumnya. Atribut turunan ini menyediakan bentuk agregasi dari data transaksi. Seperti yang telah disebutkan, dalam dataset kami hanya terdapat dua atribut numerik, yaitu jumlah mata uang asing dan jumlah mata uang lokal. Atribut lainnya bersifat kategorikal. Oleh karena itu, seperti dalam, kami membuat atribut turunan untuk setiap transaksi dalam dataset guna menempatkan transaksi kartu kredit tersebut dalam konteks historis perilaku belanja sebelumnya.

Tabel 1. Presentasi transaksi katu kredit berdasarkan jenis transaksi

Transaction types	Dataset U	Dataset A
Retail purchase	48.65	94.67
Disputed transaction	15.58	0.00
Non-directed payment	14.15	0.50
Retail payment	8.85	0.00
Miscellaneous fees	4.11	0.00
Transaction code	3.91	0.00
Cash-Write-Off-Debt	1.30	0.00
Cash-Adv-Per-Fee	0.62	0.00
Check-Item	0.63	4.54
Retail-Adjust	0.01	0.00
Others	2.19	0.29
Total	100.00	100.00

2.2. Data *Preprocessing*

Kita memerlukan data berkualitas tinggi untuk menghasilkan hasil data mining yang berkualitas tinggi. Terdapat banyak faktor yang menentukan kualitas data, termasuk akurasi, kelengkapan, dan konsistensi. Oleh karena itu, kita perlu menerapkan pra-pemrosesan data (data preprocessing) terlebih dahulu sebelum mengembangkan proses data mining utama [14].



Gambar 3. Bentuk-bentuk Prapemrosesan Data

Gambar 3 Langkah-langkah utama dalam data preprocessing meliputi pembersihan data (data cleaning), integrasi data (data integration), reduksi data (data reduction), dan transformasi data (data transformation).
Tugas data cleaning adalah untuk "membersihkan" data dengan cara mengisi nilai yang hilang, menghaluskan data yang bising (noisy), mengidentifikasi atau menghapus outlier, dan menyelesaikan inkonsistensi data [15].

Untuk mengisi nilai yang hilang, kita dapat memilih salah satu dari metode berikut; (1)Mengabaikan tuple (digunakan ketika label kelas hilang), (2)Mengisi nilai yang hilang secara manual, (3)Menggunakan konstanta global untuk mengisi nilai yang hilang (misalnya mengganti semua nilai atribut yang hilang dengan label seperti "Tidak Diketahui"), (4)Menggunakan ukuran pemusatan data (seperti rata-rata atau median) dari atribut tersebut untuk mengisi nilai yang hilang, (5)Menggunakan rata-rata atau median atribut untuk semua sampel yang termasuk dalam kelas yang sama dengan tuple tersebut (contohnya, jika kita mengklasifikasikan pelanggan berdasarkan risiko kredit, kita dapat mengganti nilai pendapatan yang hilang dengan nilai rata-rata pendapatan dari pelanggan yang memiliki kategori risiko kredit yang sama. Jika distribusi data untuk kelas tersebut condong (skewed), maka median merupakan pilihan yang lebih baik), (6)Menggunakan nilai yang paling mungkin untuk mengisi nilai yang hilang (nilai ini dapat ditentukan dengan metode regresi, alat berbasis inferensi dengan pendekatan Bayesian, atau *decision tree induction*) [16].

2.3. *Support Vector Machines* (SVM)

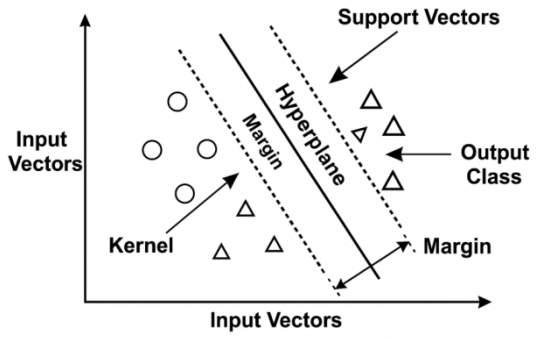
Support Vector Machines (SVM) adalah teknik pembelajaran statistik yang telah terbukti sangat berhasil dalam berbagai tugas klasifikasi. Beberapa karakteristik unik dari algoritma ini menjadikannya sangat cocok untuk masalah klasifikasi biner, seperti deteksi penipuan. SVM merupakan klasifikator linear yang bekerja dalam ruang fitur berdimensi tinggi**,** yang merupakan hasil pemetaan non-linear dari ruang input permasalahan yang sedang ditangani [4,5].

Keuntungan bekerja dalam ruang fitur berdimensi tinggi adalah bahwa pada banyak kasus, tugas klasifikasi non-linear di ruang input asli menjadi tugas klasifikasi linear di ruang fitur berdimensi tinggi tersebut. SVM dapat bekerja di ruang fitur berdimensi tinggi tanpa menambah kompleksitas komputasi.

Kesederhanaan klasifikator linear dan kemampuannya bekerja di ruang yang kaya fitur membuat SVM menarik untuk digunakan dalam

P-ISSN : 2089-3353
E-ISSN : 2808-9162

tugas deteksi penipuan**,** di mana ketidakseimbangan data (antara kasus penipuan dan bukan penipuan) membuat ekstraksi fitur yang bermakna menjadi sangat penting dan sulit dilakukan. Aplikasi SVM mencakup bidang-bidang seperti bioinformatika**,** penglihatan mesin (*machine vision*)**,** kategorisasi teks**,** dan analisis deret waktu (*time series*) [14].



Gambar 4. *Unit Support Vector Machines* (SVM)

Gambar 4 menunjukkan prinsip dasar *Support Vector Machine* (SVM) sebagai algoritma klasifikasi. SVM bekerja dengan menentukan *hyperplane* optimal yang berfungsi memisahkan data ke dalam dua kategori berbeda. Garis pemisah ini ditentukan oleh titik-titik data terdekat dari masing-masing kelas yang disebut support vectors. Jarak antara hyperplane dan support vectors dinamakan margin, dan SVM berupaya memaksimalkan jarak ini agar pemisahan antar kelas lebih optimal. Jika data tidak dapat dipisahkan secara linear, digunakan fungsi kernel untuk memproyeksikan data ke dimensi yang lebih tinggi sehingga memungkinkan terbentuknya hyperplane. Dengan pendekatan tersebut, SVM dapat mengklasifikasikan data baru secara lebih akurat berdasarkan posisinya terhadap hyperplane.

Dalam SVM, fungsi klasifikasi adalah bidang hiper yang memisahkan kelas data yang berbeda.

$$\langle w, x \rangle + b = 0 \qquad (1)$$

Fungsi klasifikasi memiliki representasi ganda sebagai berikut, dimana yi adalah label klasifikasi dari titik data masukan.

$$\sum_i \; aiyi \langle xi, x \rangle + b = 0 \qquad (2)$$

Dengan menggunakan fungsi kernel k, fungsi klasifikasi dual di atas dalam ruang berdimensi tinggi H dapat ditulis sebagai.

$$\sum_i \; aiyik \langle x1, x \rangle + b = 0 \qquad (3)$$

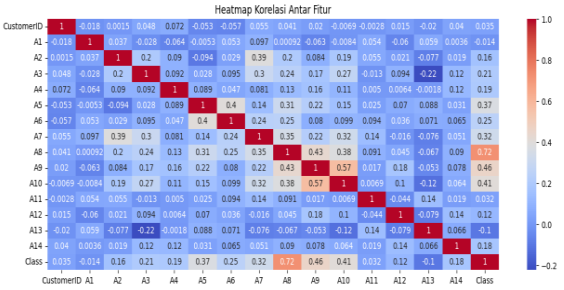
Sebagaimana disebutkan sebelumnya, dalam SVM, fungsi klasifikasi terbaik adalah bidang hiper yang memiliki margin maksimum yang memisahkan kelas-kelas. Permasalahan menemukan bidang hiper dengan margin maksimal dapat dirumuskan sebagai masalah pemrograman kuadrat.[14]

2.4. Random forest

Pada penelitian ini, LSTM dengan parameter yang telah dioptimasi digunakan untuk meramalkan harga saham dengan menggunakan kerangka kerja optuna. Kami menguji sejumlah hyperparameter dengan beberapa arsitektur LSTM, termasuk pengoptimal (SGD, Adagrad, RMSprop, Nadam, Adamax, dan Adam), unit tersembunyi LSTM, tingkat dropout, epoch, ukuran batch, dan learning rate Popularitas model pohon keputusan dalam data mining berasal dari kemudahan penggunaannya, fleksibilitas dalam menangani berbagai jenis atribut data, dan kemudahan interpretasi [17].

Namun, model pohon tunggal dapat tidak stabil dan sangat sensitif terhadap data pelatihan tertentu. Metode ensemble bertujuan untuk mengatasi masalah ini dengan mengembangkan sekumpulan model dan menggabungkan prediksi mereka untuk menentukan label kelas dari suatu data. Random forest adalah model ensemble dari pohon klasifikasi (atau regresi).

Ensemble bekerja dengan baik saat masing-masing model anggotanya berbeda satu sama lain, dan random forest mencapai variasi antar pohon dengan dua sumber acak, pertama, setiap pohon dibangun dari sampel pelatihan yang di-bootstrap (yaitu, diambil secara acak dengan pengembalian dari data pelatihan). Kedua, hanya sebagian kecil atribut yang dipilih secara acak yang dipertimbangkan di setiap node saat membangun pohon.[8,10,11]



Gambar 5. Heatmap Korelasi Antar Fitur

Gambar ini menunjukkan heatmap dari matriks korelasi yang menggambarkan hubungan antara fitur (variabel) dalam dataset.

Nilai korelasi berkisar dari -1 sampai +1:
1) +1 → hubungan positif sempurna (jika satu naik, yang lain ikut naik).
2) 0 → tidak ada hubungan linear.
3) -1 → hubungan negatif sempurna (jika satu naik, yang lain turun).

Dalam gambar:
1) Warna merah menunjukkan korelasi tinggi positif.
2) Warna biru menunjukkan korelasi mendekati nol atau negatif.
Interpretasi Nilai Korelasi:

Author : **Tasya Ramadani[1)], Crystian Delopinli.S[2)], Raffi Septiawan[3)], Edi Ismanto[4)]**

P-ISSN : 2089-3353
E-ISSN : 2808-9162

1) Diagonal (nilai = 1), semua fitur memiliki korelasi sempurna dengan dirinya sendiri, ditandai dengan warna merah pekat (nilai = 1). Ini normal.

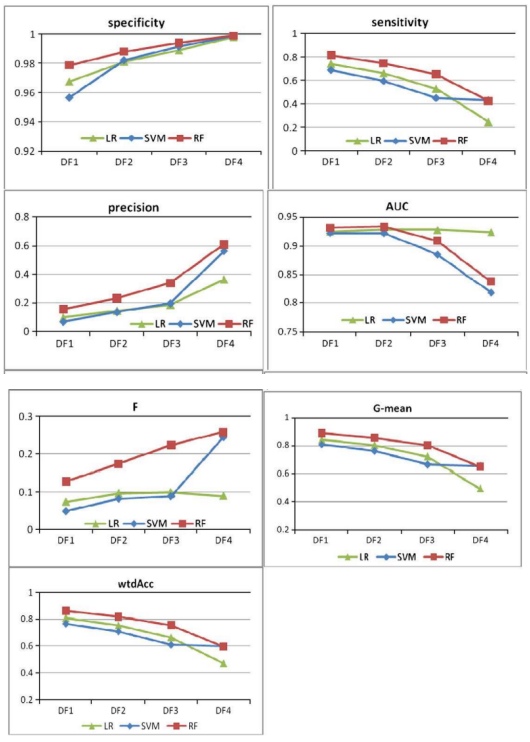
2) Korelasi antar fitur, sebagian besar fitur (A1–A14) memiliki korelasi rendah satu sama lain (warna biru muda hingga biru tua, nilai < 0.3). Hal ini menunjukkan bahwa fitur-fitur relatif independen, sehingga tidak banyak redundansi antar variabel.

3) Fitur yang cukup berkorelasi, terlihat beberapa pasangan fitur dengan korelasi menengah, misalnya A9–A10 (0.57) dan A8–A9 (0.35). Korelasi ini berarti ada informasi yang agak mirip, tetapi tidak terlalu kuat sehingga masih bisa saling melengkapi.

4) Hubungan dengan Target (Class), korelasi antara Class (fraud/tidak fraud) dengan fitur masih relatif rendah, misalnya A8 (0.42) dan A14 (0.19). Artinya, tidak ada satu fitur tunggal yang sangat dominan untuk mendeteksi fraud, sehingga algoritma machine learning perlu menggabungkan banyak fitur untuk meningkatkan akurasi.

Dengan demikian, random forest menggabungkan konsep;(1)Bagging, yaitu membuat model-model individu dalam ensemble melalui pengambilan sampel acak (dengan pengembalian) dari data pelatihan, dan (2)Metode subruang acak (random subspace), yaitu membangun setiap pohon dari subset atribut yang dipilih secara acak [11].

3. Hasil dan Pembahasan



Gambar 6. Performa di Berbagai Tingkat Penipuan Dalam Data Pelatihan

Gambar 6 menampilkan grafik perbandingan antara teknik-teknik di berbagai dataset pelatihan, pada berbagai ukuran kinerja. Akurasi pada kasus non-fraud, seperti yang diberikan oleh spesifisitas, sangat tinggi, dengan RF menunjukkan kinerja yang lebih baik secara keseluruhan. Seperti yang diharapkan, spesifisitas meningkat dengan tingkat penipuan yang lebih rendah pada data pelatihan, karena semakin banyak kasus yang diklasifikasikan ke dalam kelas mayoritas. Seperti yang dicatat sebelumnya, akurasi pada kasus penipuan lebih penting untuk aplikasi pendeteksi penipuan, dan sensitivitas di sini terlihat menurun dengan tingkat penipuan yang lebih rendah pada data pelatihan untuk semua teknik; regresi logistik, bagaimanapun, menunjukkan akurasi yang sangat rendah ketika tingkat penipuan pada data pelatihan berada pada tingkat terendah (DF4, 2% penipuan). RF sekali lagi menunjukkan kinerja terbaik, diikuti oleh LR dan kemudian SVM; untuk dataset pelatihan dengan tingkat penipuan terendah, bagaimanapun, SVM melampaui LR dan berkinerja sebanding dengan RF.

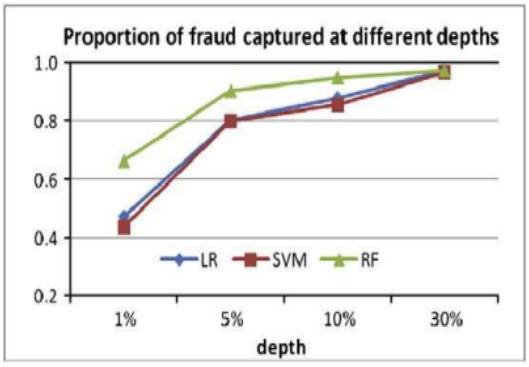
Pola ini, dengan SVM yang menyamai kinerja RF ketika dilatih dengan proporsi terendah dari kasus penipuan dalam data, juga terlihat untuk ukuran lainnya. Presisi meningkat dengan tingkat penipuan yang lebih rendah dalam data pelatihan dengan lebih sedikit kasus yang diklasifikasikan sebagai penipuan, akurasi prediksi penipuan tersebut meningkat. Di sini, sekali lagi, RF menunjukkan kinerja tertinggi; SVM dan LR memiliki kinerja yang serupa, kecuali untuk DF4, di mana kinerja SVM mendekati kinerja RF. Pada F-measure, yang menggabungkan tradeoff antara akurasi pada kasus penipuan dan ketepatan dalam memprediksi penipuan, RF menunjukkan kinerja yang jauh lebih baik dengan tingkat penipuan terendah pada data pelatihan (DF4), SVM memiliki kinerja yang sebanding dengan RF, dan LR jauh lebih rendah. Performa pada ukuran G-mean dan wtdAcc, yang mengambil pertimbangan gabungan antara akurasi pada kasus fraud dan non-fraud, mirip dengan sensitivitas.

Kinerja LR patut dicatat pada ukuran AUC sementara baik RF maupun SVM menunjukkan penurunan AUC dengan tingkat penipuan yang lebih rendah pada data pelatihan, LR terlihat mempertahankan kinerja yang baik secara konsisten. AUC, tidak seperti ukuran kinerja lainnya di sini, tidak bergantung pada ambang batas klasifikasi. Dengan demikian, ketika ambang batas ini tidak relevan, model LR dari data pelatihan yang berbeda menunjukkan kinerja AUC yang serupa. Perhatikan bahwa kasus-kasus penipuan di seluruh dataset pelatihan yang berbeda adalah sama, dengan hanya kasus-kasus non-penipuan yang diambil sampelnya secara berbeda untuk mendapatkan tingkat penipuan yang berbeda dalam data pelatihan. Nilai AUC yang tinggi secara

Author : **Tasya Ramadani[1)], Crystian Delopinli.S[2)], Raffi Septiawan[3)], Edi Ismanto[4)]**

P-ISSN : 2089-3353
E-ISSN : 2808-9162

konsisten untuk LR di seluruh dataset pelatihan menunjukkan bahwa model LR mempertahankan peringkat kasus yang sama, terlepas dari tingkat undersampling kasus non-fraud dalam data pelatihan [13,14].



Gambar 7. Proporsi Kasus Penipuan Yang Tertangkap Pada Kedalaman File Yang Berbeda (Data Pelatihan DF2)

Gambar 7 menunjukkan proporsi kasus penipuan yang ditangkap pada kedalaman 1%, 5%, 10% dan 30% untuk model yang dilatih pada dataset DF2 (memiliki tingkat penipuan 10%). RF terlihat menangkap lebih banyak kasus penipuan, dengan SVM dan LR menunjukkan kinerja yang serupa. Dengan semua teknik mendeteksi lebih banyak kasus penipuan dengan kedalaman yang semakin meningkat, perbedaan antara RF dan teknik lainnya secara bertahap berkurang. RF mengidentifikasi sekitar 90% kasus penipuan pada data uji dengan kedalaman 5%, sedangkan SVM dan LR mengidentifikasi 80%. Pada kedalaman 30%, sebagian besar kasus penipuan ditangkap oleh semua Teknik [3].

Secara umum, semua teknik menunjukkan kemampuan yang cukup baik dalam memodelkan penipuan pada data yang digunakan. Namun, kinerja bervariasi tergantung pada teknik yang digunakan dan ukuran performa yang dipilih**.** Sensitivity**,** G-mean**,** dan Weighted Accuracy menurun seiring dengan menurunnya proporsi kasus penipuan dalam data pelatihan. Sebaliknya, Precision dan Specificity justru meningkat. Untuk F-measure dan AUC**,** Logistic Regression mampu mempertahankan kinerja yang stabil meskipun proporsi penipuan dalam data pelatihan bervariasi. Random Forest dan SVM menunjukkan penurunan AUC dan peningkatan F-measure [6].

Dari sudut pandang implementasi dan aplikasi nyata, tingkat penangkapan penipuan (fraud capture rate) pada kedalaman file yang berbeda lebih informatif. Random Forests menunjukkan kinerja yang jauh lebih tingkat penangkapan penipuan (*fraud capture rate)* pada kedalaman atas file (misalnya top 1%–5%). Artinya, RF mampu menangkap lebih banyak kasus penipuan dengan false positive yang lebih sedikit**,** yang sangat penting dalam penerapan nyata. Logistic Regression menunjukkan kinerja yang konsisten pada berbagai tingkat undersampling. SVM justru meningkat kinerjanya di kedalaman atas ketika proporsi kasus penipuan dalam data pelatihan semakin kecil [9,10].

4. Kesimpulan

Seiring dengan meningkatnya transaksi bisnis kartu kredit, kasus penipuan juga semakin meningkat. Jelas, jaringan global memberikan peluang baru bagi penjahat sebanyak yang diberikan bagi bisnis. Meskipun menawarkan banyak keuntungan dan membuka saluran baru untuk transaksi bisnis, internet juga meningkatkan kemungkinan terjadinya penipuan dalam transaksi kartu kredit. Berita baiknya adalah teknologi untuk mencegah penipuan kartu kredit juga terus berkembang secara signifikan seiring berjalannya waktu.

Penurunan biaya komputasi membantu dalam pengembangan sistem kompleks yang dapat menganalisis transaksi penipuan dalam hitungan detik. Sama pentingnya adalah mengidentifikasi segmen transaksi yang tepat yang harus diperiksa, karena tidak semua transaksi memiliki tingkat risiko yang sama. Menemukan keseimbangan optimal antara ‘biaya total penipuan’ dan langkah-langkah lain yang dijelaskan dalam artikel ini dapat membantu bank penerbit dan bank penerima dalam memerangi penipuan dengan lebih efisien. Dengan demikian, model penambangan data yang diusulkan mampu meningkatkan kinerja dan mendukung pekerjaan analis kredit. Pemilihan fitur-fitur penting merupakan tantangan tersendiri. Dalam penelitian selanjutnya, kami berencana untuk melakukan beberapa metode pemilihan fitur untuk mengetahui metode mana yang dapat memberikan kinerja klasifikasi terbaik.

Daftar Rujukan

[1] T. P. Bhatla, V. Prabhu, and A. Dua, “Understanding Credit Card Frauds,” Cards Bus. Rev., vol. 1, no. 6, pp. 1–15, 2003.
[2] R. Bin Sulaiman, V. Schetinin, and P. Sant, “Review of Machine Learning Approach on Credit Card Fraud Detection,” Human-Centric Intell. Syst., vol. 2, no. 1–2, pp. 55–68, 2022, doi: 10.1007/s44230-022-00004-0.
[3] K. SaThierbach et al., "Analysis of health-related indicators in home-dwelling elderly using covariance structure analysis," Proc. Natl. Acad. Sci., vol. 3, no. 1, pp. 1–15, 2015. [Online]. Available: http://dx.doi.org/10.1016/j.bpj.2015.06.056/j.str.2013.02.005%0Ahttp://dx.doi.org/10.10
[4] M. Zhu, Y. Zhang, Y. Gong, C. Xu, and Y. Xiang, “Enhancing Credit Card Fraud Detection: A Neural Network and SMOTE Integrated Approach,” J. Theory Pract. Eng. Sci., vol. 4, no. 02, pp. 23–30, 2024, doi: 10.53469/jtpes.2024.04(02).04.
[5] S. Sruthi, S. Emadaboina, and C. Jyotsna, “Enhancing Credit Card Fraud Detection with Light Gradient-Boosting Machine: An Advanced Machine Learning Approach,” 2024 Int. Conf. Knowl. Eng. Commun. Syst. ICKECS 2024, 2024, doi: 10.1109/ICKECS61492.2024.10616809.
[6] I. D. Mienye and N. Jere, “Deep Learning for Credit Card Fraud

P-ISSN : 2089-3353
E-ISSN : 2808-9162

Detection: A Review of Algorithms, Challenges, and Solutions," IEEE Access, vol. 12, no. July, pp. 96893–96910, 2024, doi: 10.1109/ACCESS.2024.3426955.

[7] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," Decis. Support Syst., vol. 50, no. 3, pp. 602–613, 2011, doi: 10.1016/j.dss.2010.08.008.

[8] E. D. Madyatmadja and M. Aryuni, "Comparative study of data mining model for credit card application scoring in bank," J. Theor. Appl. Inf. Technol., vol. 59, no. 2, pp. 269–274, 2014.

[9] 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.

[10] A. Cherif, A. Badhib, H. Ammar, S. Alshehri, M. Kalkatawi, and A. Imine, "Credit card fraud detection in the era of disruptive technologies: A systematic review," J. King Saud Univ. - Comput. Inf. Sci., vol. 35, no. 1, pp. 145–174, 2023, doi: 10.1016/j.jksuci.2022.11.008.

[11] S. Chakravorti and T. To, "A theory of credit cards," Int. J. Ind. Organ., vol. 25, no. 3, pp. 583–595, 2007, doi: 10.1016/j.ijindorg.2006.06.005.

[12] M. Abdul Salam, K. M. Fouad, D. L. Elbably, and S. M. Elsayed, "Federated learning model for credit card fraud detection with data balancing techniques," Neural Comput. Appl., vol. 36, no. 11, pp. 6231–6256, 2024, doi: 10.1007/s00521-023-09410-2.

[13] I. D. Mienye and Y. Sun, "A Deep Learning Ensemble With Data Resampling for Credit Card Fraud Detection," IEEE Access, vol. 11, no. February, pp. 30628–30638, 2023, doi: 10.1109/ACCESS.2023.3262020.

[14] E. Ileberi, Y. Sun, and Z. Wang, "A machine learning based credit card fraud detection using the GA algorithm for feature selection," J. Big Data, vol. 9, no. 1, 2022, doi: 10.1186/s40537-022-00573-8.

[15] E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba, and G. Obaido, "A Neural Network Ensemble with Feature Engineering for Improved Credit Card Fraud Detection," IEEE Access, vol. 10, pp. 16400–16407, 2022, doi: 10.1109/ACCESS.2022.3148298.

[16] J. K. Afriyie et al., "A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions," Decis. Anal. J., vol. 6, no. November 2022, p. 100163, 2023, doi: 10.1016/j.dajour.2023.100163.

[17] B. Chugh, N. Malik, D. Gupta, and B. S. Alkahtani, "A probabilistic approach driven credit card anomaly detection with CBLOF and isolation forest models," Alexandria Eng. J., vol. 114, no. October 2024, pp. 231–242, 2025, doi: 10.1016/j.aej.2024.11.054.