TESIS

FRAUD DETECTION SYSTEM MENGGUNAKAN SVM, RF, KNN DENGAN VOTING CLASSIFIER pada AUTOMATIC TELLER MACHINE

(Studi Kasus: Bank Sultra Cabang Pembantu Sao–Sao)

Disusun oleh

NAMA	**: CHLYFEN RICHARD SALIBANA**
NIM	**: 24.55.1581**
Konsentrasi	**: Business Intelligence**

FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2026

TESIS

FRAUD DETECTION SYSTEM MENGGUNAKAN SVM, RF, KNN DENGAN VOTING CLASSIFIER pada AUTOMATIC TELLER MACHINE

(Studi Kasus: Bank Sultra Cabang Pembantu Sao–Sao)

FRAUD DETECTION SYSTEM USING SVM, RF, KNN, WITH VOTING CLASSIFIER an AUTOMATIC TELLER MACHINE

(Case Study: Bank Sultra, Sao-Sao Branch)

Diajukan untuk memenuhi salah satu syarat mencapai derajat Pascasarjana

Program Studi Sekolah Pascasarjana PJJ S2 Informatika

Disusun oleh

NAMA	**: CHLYFEN RICHARD SALIBANA**
NIM	**: 24.55.1581**
Konsentrasi	**: Business Intelligence**

FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2026

HALAMAN PERSETUJUAN

FRAUD DETECTION SYSTEM MENGGUNAKAN SVM, RF, KNN DENGAN VOTING CLASSIFIER pada AUTOMATIC TELLER MACHINE

FRAUD DETECTION SYSTEM USING SVM, RF, KNN WITH VOTING CLASSIFIER an AUTOMATIC TELLER MACHINE

yang disusun dan diajukan oleh

Chlyfen Richard Salibana

24.55.1581

Telah disetujui oleh Tim Dosen Pembimbing Tesis
pada tanggal 04 Maret 2026

Pembimbing

Prof. Dr. Ema Utami, S.Si., M.Kom.
NIK. 190302073

HALAMAN PENGESAHAN

FRAUD DETECTION SYSTEM MENGGUNAKAN SVM, RF, KNN, DENGAN VOTING CLASSIFIER pada AUTOMATIC TELLER MACHINE

FRAUD DETECTION SYSTEM USING SVM, RF, KNN, WITH VOTING CLASSIFIER an AUTOMATIC TELLER MACHINE

yang disusun dan diajukan oleh

Chlyfen Richard Salibana
24.55.1581

Telah dipertahankan di depan Dewan Penguji
pada tanggal 04 Maret 2026

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Alva Hendi Muhammad,S.T.,M.Eng.,Ph.D. **NIK. 190302493**	
Dhani Ariatmanto,S.T.,M.Eng.,Ph.D. **NIK. 190302001**	
Prof. Dr. Ema Utami,S.Si.,M.Kom. **NIK. 190302037**	

Tesis ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Magister Komputer
Tanggal 04 Maret 2026

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN TESIS

Yang bertandatangan di bawah ini,

Nama mahasiswa : Chlyfen Richard Salibana
NIM : 24.55.1581

Menyatakan bahwa Tesis dengan judul berikut:

Fraud Detection System Menggunakan SVM, RF, KNN, dengan VOTING CLASSIFIER pada Automatic Teller Machine

Dosen Pembimbing: Prof. Dr. Ema Utami, S.Si., M. Kom.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 04 Maret 2026

Yang Menyatakan,

Chlyfen Richard Salibana

HALAMAN PERSEMBAHAN

Tesis ini dengan penuh rasa syukur dan cinta saya persembahkan untuk istri saya tercinta,yang senantiasa hadir sebagai sumber kekuatan, doa, dan semangat di setiap langkah perjalanan studi ini. Terima kasih atas kesabaranmu menunggu, pengertianmu di saat lelah, serta dukungan tanpa henti yang engkau berikan dalam suka maupun duka. Setiap halaman dari karya ini adalah jejak dari pengorbanan, doa, dan cinta tulusmu yang tidak ternilai. Semoga pencapaian ini menjadi awal dari kebaikan-kebaikan lain yang dapat kita raih dan nikmati bersama di masa yang akan datang.

KATA PENGANTAR

Puji syukur ke hadirat Tuhan Yang Maha Esa atas limpahan Rahmat dan Karunia-Nya sehingga penulis dapat menyelesaikan tugas akhir ini yang berjudul **"Fraud Detection System Menggunakan SVM, RF, KNN, dengan Voting Classifier pada Automatic Teller Machine"** sebagai salah satu syarat untuk memperoleh gelar Magister Informatika pada Program Studi Magister Informatika, Universitas Amikom Yogyakarta. Penelitian ini membahas pengembangan sistem deteksi kecurangan pada transaksi Automatic Teller Machine (ATM) dengan membandingkan beberapa algoritma klasifikasi dan pendekatan ensemble untuk meningkatkan akurasi deteksi fraud.

Terselesaikannya tesis ini tidak terlepas dari bantuan, dukungan, dan bimbingan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis menyampaikan terima kasih yang sebesar-besarnya kepada:

- Prof. Dr. Ema Utami, S.Si., M.Kom. selaku dosen pembimbing yang telah memberikan bimbingan, arahan, ilmu, serta motivasi mulai dari perencanaan hingga penyusunan akhir tesis ini.
- Pimpinan dan segenap sivitas akademika Universitas Amikom Yogyakarta, khususnya di lingkungan Program Studi Magister Informatika, yang telah memberikan ilmu, fasilitas, dan suasana akademik yang kondusif selama masa studi.
- Rekan-rekan mahasiswa Magister Informatika yang senantiasa memberikan dukungan, diskusi, serta masukan yang konstruktif dalam proses penelitian ini.

- Istri tercinta yang selalu memberikan doa, semangat, dan dukungan sehingga penulis dapat menyelesaikan studi tepat waktu.

Penulis menyadari bahwa tesis ini masih jauh dari sempurna, baik dari segi isi maupun penyajian, karena keterbatasan pengetahuan dan pengalaman. Oleh sebab itu, penulis sangat mengharapkan kritik dan saran yang membangun demi penyempurnaan karya ilmiah ini di masa yang akan datang. Semoga tesis ini dapat memberikan manfaat bagi pengembangan ilmu pengetahuan di bidang sistem deteksi kecurangan, khususnya pada transaksi ATM, serta menjadi referensi bagi peneliti dan praktisi yang tertarik dalam penerapan algoritma machine learning untuk keamanan transaksi finansial.

Yogyakarta, 04 Maret 2026

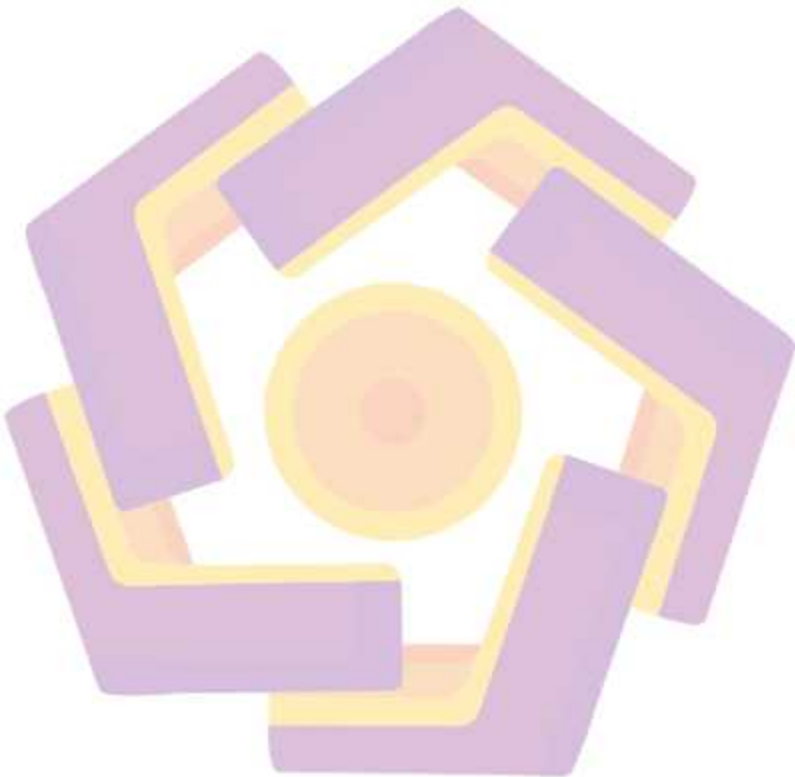
Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN



DAFTAR LAMBANG DAN SINGKATAN

Lambang/ Singkatan	Keterangan
ApJII	Asosiasi Penyelenggara Jasa Internet Indonesia
AI	*Artificial Intelligence*
ML	*Machine Learning*
BPD	Bank Pembangunan Daerah
MoU	*Memorandum of Understanding*
SVM	*Support Vector Machine*
RF	*Random Forest*
K-NN	*K-Nearest Neighbors*
CART	*Classification and Regression Tree*
SMOTE	*synthetic minority over-sampling technique*
ATM	*Automatic Teller Machine*
SPPK	Sistem Pendukung Pengambilan Keputusan
ADASYN	Adaptive Synthetic Sampling
DT	*Decision Tree*
CNP	*card-not-present*
AUC	*Area Under Curve*

DAFTAR ISTILAH

Istilah	Keterangan
Fraud	Kecurangan
AI	*Artificial Intelligence*
ML	*Machine Learning*

INTISARI

Arus globalisasi dan kemudahan komunikasi yang terintegrasi internet kini menjadi sarana yang sangat populer dan diminati banyak orang. Hal ini terlihat terutama dalam sistem transaksi elektronik, perbankan online, serta metode pembayaran digital. Adapun tujuan penelitian ini yaitu untuk menerapkan metode klasifikasi dengan menguji dan membandingkan antar model SVM, RF, K-NN, dengan *voting classifier* dalam mengembangkan, mengevaluasi dan mendeteksi transaksi kecurangan yang terjadi secara efektif menggunakan model *machine learning* (ML) pada BPD Sultra. Fokus penelitian ini untuk mengidentifikasi ciri-ciri transaksi mencurigakan berdasarkan data yang relevan dan menyusun peningkatan keamanaan transaksi. Metode dalam penelitian ini adalah kuantitatif yanng bersifat deskriptif dan eksploratif dalam perbandingan model ML yang akan di uji. Hasil penelitian menunjukkan bahwa: (1). Performa model ML SVM, RF, K-NN dengan *voting classifier* dapat mendeteksi aktivitas kecurangan pada transaksi ATM di BPD Sultra; (2). Tingkat akurasi dan metrik evaluasi dari ke tiga model ML dalam mendeteksi kecurangan pada transaksi ATM menunjukkan nilai F1-Score yang paling baik adalah model algoritmik RF yakni 99%; (3). Penerapan metode ensemble learning dengan SMOTE dapat meningkatkan performa model dibandingkan dengan model SVM, RF, K-NN tanpa *voting classifier* secara individual. Berdasarkan hasil penelitian saran yang dapat diajukan penulis sebagai berikut: (1) Penelitian selanjutnya disarankan menggunakan dataset multi-periode untuk menguji stabilitas dan konsistensi performa model terhadap variasi pola transaksi; (2) Penggunaan SMOTE dalam mensintesis data diperlukan ekplorasi alternatif seperti ADASYN atau kombinasi undersampling, oversampling untuk memvalidasi kekuatan model; dan perlu dilakukan penelitian selanjutnya untuk mengintegrasikan pendekatan hybrid antara machine learning dengan deep learning dalam mendeteksi fraud.

Kata Kunci: Machine learning; SVM; K-NN; RF; SMOTE.

ABSTRACT

The flow of globalization and the ease of communication integrated with the internet has now become a very popular and sought-after medium for many people. This is especially seen in electronic transaction systems, online banking, and digital payment methods. The purpose of this study is to apply a classification method by testing and comparing SVM, RF, K-NN models, with a voting classifier in developing, evaluating, and detecting fraudulent transactions that occur effectively using a machine learning (ML) model at BPD Sultra. The focus of this study is to identify the characteristics of suspicious transactions based on relevant data and develop transaction security improvements. The method in this study is quantitative, descriptive, and exploratory in comparing the ml models to be tested. The results of the study show that: (1). The performance of the ml models SVM, RF, K-NN with a voting classifier can detect fraudulent activity in atm transactions at BPD Sultra; (2). The level of accuracy and evaluation metrics of the three ml models in detecting fraud in atm transactions show that the best F1-Score value is the rf algorithmic model, namely 99%; (3). The application of the ensemble learning method with smote can improve model performance compared to the SVM, RF, KNN models without individual classifier voting. Based on the research results, the suggestions that the author can put forward are as follows: (1) further research is recommended to use multi-period datasets to test the stability and consistency of model performance against variations in transaction patterns; (2) the use of smote in synthesizing data requires alternative exploration such as adasyn or a combination of undersampling, oversampling to validate the strength of the model; and further research is needed to integrate a hybrid approach between machine learning and deep learning in detecting fraud.

Keywords: *Machine learning; SVM; K-NN; RF; SMOTE.*

BAB 1

PENDAHULUAN

1.1. Latar Belakang

Ilmu pengetahuan dan teknologi yang terus berkembang pesat, ditopang oleh dampak globalisasi, memberikan pengaruh yang signifikan dalam kehidupan kita. Kemajuan ini telah menghadirkan berbagai kemudahan dalam aktivitas sehari-hari, bahkan menjangkau ruang pribadi individu. Dengan arus globalisasi dan kemudahan komunikasi yang terintegrasi, internet kini menjadi sarana yang sangat populer dan diminati banyak orang. Kehadiran fasilitas internet membuat dunia terasa semakin kecil dan dekat. Hal ini terutama terlihat dalam sistem transaksi elektronik, perbankan online, serta metode pembayaran digital (Hasanah & Basarah, 2023). Termasuk dalam pola transaksi yang telah mengalami banyak inovasi dan variasi, seiring dengan perkembangan fasilitas telekomunikasi dan perangkat teknologi informasi yang canggih. Hal ini mendukung pentingnya informasi sebagai elemen utama dalam memenuhi kebutuhan yang ada.

Seiring dengan kemajuan ini, risiko kejahatan siber, terutama dalam bentuk penipuan transaksi, juga meningkat secara signifikan. Hal ini memberikan dampak penggunaan kartu yang sangat tinggi terutama dalam bertransaksi membeli dan membayar kebutuhan. Hal ini menjadi dasar dalam terjadinya kasus penipuan yang semakin tinggi. Sehingga sangat diperlukan algoritma yang efektif, aman dan efisien untuk dikembangkan dalam mencegah serta meminimalisir fraud yang terjadi selama melakukan transaksi (RB & KR, 2021). Hal ini juga menjadi bagian terpenting untuk dapat melakukan pengamatan dasar sekaligus meningkatkan

system keamanan dalam penggunaan kartu untuk bertransaksi dengan nyaman serta dapat meningkatkan kepercayaan dari nasabah (Madhurya et al., 2022).

Menurut informasi dari Asosiasi Penyelenggara Jasa Internet Indonesia (ApJII) dan Bank Indonesia, jumlah kasus transaksi mencurigakan yang berkaitan dengan penipuan terus mengalami peningkatan setiap tahunnya. Dalam hal ini mengungkapkan bahwa dari November 2024 hingga 28 Desember 2025, tercatat 411.055 laporan penipuan di *Indonesia Scam Skate Center*, dengan 681.890 rekening yang terverifikasi terlibat dalam fraud dan scam. Hal ini menjadi tantangan besar bagi perusahaan dan lembaga keuangan dalam menjaga keamanan transaksi para pelanggan (Hapsari & Pambayun, 2023). Salah satu tantangan utama dalam mendeteksi transaksi mencurigakan adalah keterbatasan kemampuan manusia untuk melakukan pemantauan secara terus-menerus selama 24 jam sehari. Dengan volume data transaksi yang sangat besar dan pola yang kompleks, pengawasan manual seringkali menjadi tidak efisien dan mudah terjebak dalam kesalahan. Akibatnya, banyak transaksi penipuan yang tidak terdeteksi atau terlambat dikenali, yang dapat menimbulkan kerugian finansial yang signifikan bagi perusahaan maupun individu.

Berbagai sektor industri membutuhkan kecerdasan buatan untuk mengembangkan sistem yang efektif dan efisien. Di samping itu, dengan dukungan Artificial Intelligence (AI) dan model Machine Learning (ML), pemahaman manusia tentang sistem yang rumit dapat ditingkatkan untuk membantu manusia (Nur & Nurul, 2024). Teknologi ML telah muncul sebagai solusi yang menjanjikan dalam mendukung sistem deteksi penipuan. Algoritma ML memiliki kemampuan

untuk menganalisis data transaksi secara real-time, sehingga dapat mengidentifikasi pola-pola yang tidak biasa dan menemukan karakteristik transaksi mencurigakan yang mungkin terlewatkan oleh pengawasan manusia. Dengan kemampuan adaptasi yang tinggi terhadap data yang terus berubah, teknologi ini berpotensi meningkatkan akurasi dalam mendeteksi penipuan (Rahmadani et al., 2023).

Berdasarkan penelitian yang telah dilakukan sebelumnya untuk mendeteksi kecurangan dan skimming yang terjadi pada bank diluar negeri termasuk di negeria dan india. Ini menunjukkan bahwa Cybercrime berdampak negatif besar pada ekonomi digital Nigeria menyebabkan kerugian finansial sekitar US$32 juta, sehingga menurunkan kepercayaan investor dan menghambat pertumbuhan ekonomi digital (Margaret, 2023). Sedangkan di India sendiri menunjukkan bahwa Skala Kejahatan Siber periode 2024-2025 sekitar US$6,2 miliar (Rai & Thapa, 2024). Hal ini menjadi dasar untuk dapat menerapkan dan melakukan penelitian ini di sektor perbankan Indonesia yang masih sering mengalami kecurangan (*fraud*), seperti *phising* maupun *scam*.

Bank pembangunan daerah (BPD) adalah Salah satu bank yang beroperasi menjadi pusat pertukaran ekonomi. Dalam penelitian yang dilakukan oleh (Wibisono, 2023) menyatakan bahwa BPD dapat menjaga stabilitas usaha, meningkatkan daya saing dan kinerja keuangan perbankan, seperti penerapan prinsip-prinsip tata kelola Perusahaan yang baik. Dilansir dari halaman web Bank Sultra yang di rilis pada 12 November 2021, menyatakan bahwa untuk antisipasi kejahatan perbankan seperti fraud manajemen Bank Sultra menyikapinya dengan menggaet Kejaksaan Tinggi (Kejati) untuk membantu mengatasi apabila didapati

bahwa telah terjadi kecurangan pada BPD Sultra. Kesepakatan ini di tandai dengan dilegitimasi penandatangan *Memorandum of Understanding* (MoU) antara direktur utama Bank Sultra dengan Kepala Kejati Sultra.

Tindak lanjut yang dilakukan ini, ternyata masih meninggalkan tantangan yang tersendiri bagi BPD Sultra untuk mengatasi fraud yang terjadi secara langsung di dalam system. Salah satu masalah yang menjadi pusat perhatian setelah terbitnya MoU tersebut yakni kasus skimming yang terjadi pada bulan November 2022 seperti yang dilansir dari https://validnews.id/nasional/ojk-nilai-pelaku-pembobolan-bank-sultra-tak-sendirian adanya tindakan fraud yang dilakukan oleh salah satu oknum petugas di dalam badan BPD itu sendiri menimbulkan kerugian mencapai 9 Milyar Rupiah. Kasus selanjutnya dilansir dari https://www.antarafoto.com/id/view/1826909/kasus-skimming-di-bank-sultra yang menunjukkan adanya fraud yang dilakukan oleh WNA yang membobol beberapa ATM BPD Sultra yang menimbulkan kerugian sebesar 3 Milyar Rupiah. Kasus ini terjadi tanpa sepengetahuan BPD Sultra sampai muncul adanya aduan dari nasabah yang mengalami kerugian tersebut. Hal ini disebabkan karena pada tahun tersebut monitoring fraud pada transaksi ATM masih dilakukan secara manual. Hal ini menjadi perhatian khusus yang harus dapat diselesaikan ataupun dilakukan minimalisasi untuk mengatasi serta mengetahui fraud/ kecurangan yang dapat terjadi melalui transaksi langsung oleh nasabah yang bersangkutan. Sehingga dengan peningkatan keamanan tersebut diharapkan dapat meningkatkan kepercayaan serta loyalitas nasabah kepada BPD. Kecurangan ini dapat diidentifikasi dengan salah satu metode statistik yang dapat diterapkan untuk

klasifikasi ML dengan spesifikasi menggunakan metode Support Vector Machine (SVM), Random Forest (RF), K-Nearest Neighbors (KNN), dan Voting Classifier.

Keunggulan SVM adalah kemampuannya dalam menentukan jarak menggunakan support vector, yang membuat proses komputasi menjadi lebih efisien. Penelitian yang dilakukan oleh Rustam dan rekan-rekannya pada tahun 2023 membandingkan metode K-Nearest Neighbor (KNN) dengan SVM. Hasil penelitian tersebut menunjukkan bahwa SVM memiliki kinerja yang lebih unggul, dengan keberhasilan 100% dalam mengklasifikasikan data sesuai kategori yang tepat. Selain itu, Rachman dan Purnami pada tahun 2012 juga melakukan penelitian terkait klasifikasi tingkat keganasan kanker, menerapkan metode regresi logistik dan SVM. Temuan mereka mengungkapkan bahwa akurasi SVM lebih tinggi, mencapai 98,11% (Octaviani & Yuciana, 2014).

Metode Random Forest memiliki dua fungsi untuk pemecahan suatu kasus, yaitu klasifikasi dan prediksi. Teknik dasar yang digunakan adalah pohon keputusan. Dengan kata lain metode Random Forest merupakan kumpulan pohon keputusan untuk klasifikasi dan prediksi data dengan memberikan masukan ke dalam akar di bagian atas kemudian turun ke daun di bagian bawah. Hasil analisis metode Random Forest untuk klasifikasi adalah bentuk setiap pohon dari pohon-pohon yang terbangun, sedangkan hasil prediksi diperoleh dari nilai rata-rata setiap pohon. Metode Random Forest merupakan hasil pengembangan metode Classification and Regression Tree (CART) yang menerapkan metode agregasi bagging atau bootstrap dan pemilihan fitur secara acak (Rochmawati et al., 2025) . Algoritma Random Forest mempunyai nilai m yang dapat berbeda-

beda. Nilai m merupakan banyaknya variabel prediktor yang digunakan sebagai pemisah dalam pembentukan pohon klasifikasi. Nilai m yang semakin besar akan menyebabkan korelasi yang semakin tinggi

Penelitian sebelumnya telah banyak memberikan dampak yang nyata bagi perkembangan penelitian terutama di sektor perbankan. Akan tetapi hal ini pun masih menyisakan beberapa permasalahan yang belum terselesaikan dengan baik dan teratur. K-NN memiliki kelemahan pada nilai k-fold. Agar setiap data dapat dijadikan sebagai data training dan data testing maka dibutuhkan k-fold yang merupakan salah satu metode tambahan agar dapat mensimulasikan semua data yang ada (Vika Vitaloka Pramansah, 2022). Sehingga perlu dilakukan perbandingan untuk selanjutnya dilakukan assembly dan stacking untuk meningkatkan nilai dari hasil uji yang akan dilakukan. Sedangkan SVM memiliki kekurangan dalam bentuk yang berbeda, yakni tidak dapat menganalisis data set yang mengalami tumpang tindih terutama dengan skala besar serta sangat sensitif terhadap *outlier* (Obasi et al., 2024). Kekurangan masing-masing alogritma tersebut masih menyisakan berbagai tantangan untuk segera diatasi dengan tepat guna mengurangi kesalahan yang dilakukan oleh manusia dalam mengatasi kecurangan yang terjadi dalam perbankan saat ini.

Salah satu metode ensemble populer adalah *voting classifier*, yang menggabungkan keputusan dari berbagai model klasifikasi. Metode ini terdiri dari dua jenis, *hard voting* dan *soft voting*. Pada *hard voting*, keputusan akhir diambil berdasarkan suara terbanyak dari model-model yang digunakan, sementara pada *soft voting*, keputusan diambil dengan mempertimbangkan rata-rata probabilitas

prediksi setiap model. Namun, penerapan *voting classifier* pada data tidak seimbang dapat memicu bias, karena model cenderung lebih akurat dalam memprediksi kelas mayoritas, yang mengabaikan kelas minoritas (de Oliveira et al., 2022). Oleh karena itu, untuk menangani data tidak seimbang berbagai metode telah dikembangkan, termasuk algoritma ensemble lain seperti RF, yang efektif dalam menangani ketimpangan kelas melalui pembobotan di pohon-pohon keputusan.

Selain pendekatan model, penyeimbangan data melalui teknik pengolahan seperti *synthetic minority over-sampling technique* (SMOTE) juga digunakan untuk menangani data tidak seimbang. SMOTE menghasilkan sampel sintetis bagi kelas minoritas, yang memungkinkan model untuk belajar dari data yang lebih seimbang (Basha et al., 2022). Teknik SMOTE melakukan over-sampling dengan mensintesis data kelas minoritas. Proses ini dilakukan dengan mengambil sampel dari data kelas minoritas, kemudian menciptakan sampel sintetis dengan cara interpolasi di antara sampel-sampel terdekat dari kelas minoritas (Gnip et al., 2021).

Beberapa penelitian sebelumnya yang telah disebutkan memberikan dasar penting bagi riset yang akan dilakukan ini, dan selanjutnya, peneliti akan mengacu pada literatur pendukung utama yang relevan dilakukan (Dong et al., 2021) dalam penelitian ini SVM mampu mendeteksi kecurangan yang terjadi pada produk. Fokus utama dari studi ini adalah mengembangkan model ML untuk mendeteksi penipuan. Hasil penelitian menunjukkan bahwa sejumlah besar data yang disediakan oleh basis data terlebih dahulu direkayasa menggunakan fitur tertentu. Data yang telah diproses kemudian digunakan untuk pemodelan dengan algoritma

klasifikasi SVM untuk regresi data. Hasil dari model ini kemudian dibandingkan dengan model Naive Bayes dan regresi logistik. Penelitian ini menemukan bahwa akurasi model klasifikasi SVM mencapai 98,61%. Dibandingkan dengan Naive Bayes, SVM menunjukkan kemampuan klasifikasi dan regresi yang lebih baik.

Selanjutnya (Ajay Kumar, 2024) menuliskan dalam penelitiannya mengenai implementasi SVM, Random Forest, dan KNN dalam sistem deteksi fraud, serta menyoroti keunggulan ensemble methods seperti voting classifier untuk meningkatkan akurasi dan generalisasi pada data yang kompleks dan imbalanced. Dengan perbandingan hasil yang menunjukkan bahwa Random Forest dan SVM banyak digunakan dalam sistem deteksi fraud, dengan Random Forest sering kali memberikan trade-off yang lebih baik antara precision dan recall dibanding SVM, serta menekankan pentingnya teknik balancing data seperti SMOTE. Penelitian terbaru (Ahmed et al., 2025) membahas pengembangan model ensemble (mengombinasikan beberapa algoritma termasuk KNN, RF, dan SVM) sebagai framework yang seimbang untuk klasifikasi fraud di sektor keuangan.

Berdasarkan uraian latar belakang diatas pada penelitian ini penulis tertarik untuk menerapkan metode klasifikasi dengan menguji dan membandingkan antar model SVM, RF, KNN, dengan *voting classifier* dalam mengembangkan, mengevaluasi dan mendeteksi transaksi kecurangan yang terjadi secara efektif menggunakan model *machine learning* (ML) pada Bank Pembangunan Daerah Sultra. Fokus penelitian ini adalah untuk mengidentifikasi ciri-ciri transaksi mencurigakan berdasarkan data yang relevan dan menyusun peningkatan keamanaan transaksi. Karena apabila masalah yang akan diselesaikan ini tidak

dapat selesai dengan baik, maka potensi untuk skala terjadinya fraud dalam transaksi keuangan bahkan perbankan secara spesifik akan mengalami kenaikan yang semakin tinggi setiap periode waktu tertentu. Sehingga dengan penelitian ini diharapkan akan dapat meningkatkan serta mendukung tingkat kepercayaan dari nasabah untuk melakukan transaksi dan memberikan dampak yang positif terhadap Bank Pembangunan Daerah.

1.2. Rumusan Masalah

Adapun rumusan masalah yang akan dikaji dalam penelitian riset dan pengembangan ini yaitu sebagai berikut:

a. Bagaimana performa model machine learning SVM, RF, KNN dengan *voting classifier* dalam mendeteksi aktivitas kecurangan pada transaksi ATM di Bank Pembangunan Daerah Sulawesi Tenggara?
b. Berapa tingkat akurasi dan metrik evaluasi dari model SVM, RF, KNN dengan *voting classifier* dalam mendeteksi kecurangan pada transaksi ATM?
c. Faktor apa saja yang dapat mempengaruhi performa model dalam mendeteksi transaksi yang bersifat *fraud*?
d. Apakah penerapan metode ensamble learning dapat meningkatkan performa model dibandingkan dengan model SVM, RF, KNN dengan *voting classifier* secara individual?

1.3. Batasan Masalah

Agar penelitian dapat dilaksanakan dengan fokus dan terpusat maka penulis memberikan batasan untuk kajian masalah sebagai berikut:

a. Tahap awal penelitian dilakukan proses identifikasi masalah fraud pada BPD Sultra selama periode 1 bulan yang dilanjutkan dengan studi literatur mengenai SVM, RF, KNN dengan *voting classifier*.
b. Tahap berikutnya pengumpulan dataset penelitian dari BPD Sultra dilakukan dari transaksi selama periode bulan September 2025 untuk dilakukan pengujian analisis menggunakan klasifikasi SVM, RF, KNN dengan *voting classifier*.
c. Memeriksa dataset apakah data imbalance atau tidak, jika dataset imbalance maka perlu melakukan SMOTE yaitu memilih data acak dari kelas minoritas kemudian menetapkan *k-nearest neighbours* dari data tersebut. Data sintetsis kemudian dibuat diantara data acak dan tetangga terdekat yang dipilih secara acak.
d. Penentuan nilai dan akurasi pengujian dari hasil pengujian dilakukan dengan evaluasi menggunakan *Confusion Matrix* untuk mengetahui kemampuan performa model algoritma dari *Machine Learning* (ML) yang digunakan.
e. Output hasil pengujian SVM, RF, KNN dengan *voting classifier* berupa akurasi dan nilai pasti dalam persentase yang dapat digunakan untuk deteksi seberapa tinggi kecurangan dalam system BPD Sultra.

1.4. Tujuan Penelitian

Berdasarkan rumusan masalah sebelumnya yang telah dipaparkan, sehingga ada tiga tujuan yang ingin dicapai dalam penelitian ini, yaitu:

a. Mengetahui tingkat fraud dari deteksi kecurangan yang terjadi di lingkungan Bank Pembangunan Daerah dengan menggunakan hasil uji SVM, RF, KNN dengan *voting classifier*.

b. Mengetahui tingkat akurasi pengujian menggunakan SVM, RF, KNN dengan *voting classifier* untuk system deteksi kecurangan.

c. Mengidentifikasi faktor yang mempengaruhi hasil pengujian dengan menggunakan SVM, RF, KNN dengan *voting classifier* untuk system deteksi kecurangan.

d. Mengetahui pengaruh ensemble learning terhadap tingkat akurasi pada pengujian 3 algoritma sebelumnya.

1.5. Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini:

a. Manfaat serta kontribusi ilmiah dalam ilmu pengetahuan jika penelitian ini berhasil memberikan data terbaru untuk metode perkembangan system deteksi kecurangan khususnya yang terjadi di bidang perbankan

b. Implementasi teknologi ini diharapkan dapat menjadi investasi penting dalam pengendalian dan minimalisasi tingkat kecurangan di bidang perbankan khususnya di Bank Pembangunan Daerah.

c. Dengan mengimplementasikan sistem cerdas ini tentunya akan membuka peluang riset lebih jauh lagi baik para peneliti baik dibidang perbankan maupun dibidang teknologi, dan tentunya akan melahirkan sebuah kombinasi diantara keduanya yang hasilnya akan banyak membantu kegiatan transaksi di bidang perbankan

BAB 2

TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

Penelitian yang dilakukan oleh (Eldo et al., 2024) mengkaji penerapan algoritma SVM dalam mendeteksi penipuan yang semakin kompleks dalam transaksi online. Di era digital saat ini, fenomena penipuan kerap menghadirkan tantangan besar, sebab pola-pola kecurangan terus berubah dan menjadi sangat sulit untuk diprediksi. Metode tradisional yang mengandalkan aturan statis dan sistem blacklist sering kali tidak cukup efektif, karena hanya mampu mengidentifikasi penipuan yang sesuai dengan pola yang sudah dikenal sebelumnya. Oleh karena itu, diperlukan pendekatan yang lebih dinamis dan adaptif untuk mendeteksi pola penipuan yang baru dan belum teridentifikasi. Salah satu solusi yang dapat diterapkan adalah teknik machine learning, menggunakan algoritma SVM.

Hasil penelitian menunjukkan bahwa model SVM mampu mendeteksi transaksi penipuan dengan tingkat akurasi tinggi, mencapai 95%. Selain itu, model ini juga berhasil menciptakan keseimbangan yang baik antara tingkat presisi dan recall, sehingga efektif dalam mengidentifikasi aktivitas penipuan tanpa mengabaikan transaksi yang sah. Kesimpulannya, algoritma SVM merupakan solusi yang andal untuk mendeteksi penipuan dalam transaksi online. Namun, masih diperlukan pengujian lebih lanjut pada berbagai jenis dataset untuk meningkatkan kemampuan generalisasi model ini.

(Yazid & Fiananta, 2017) memanfaatkan data dari kartu kredit yang merupakan sebuah metode pembayaran populer dan sering digunakan dalam

transaksi online. Dengan semakin banyaknya pengguna kartu kredit yang menjadikannya sebagai pilihan pembayaran sehari-hari, penting untuk meningkatkan keamanan dalam memverifikasi setiap transaksi. Hal ini terutama disebabkan oleh meningkatnya kasus penipuan dalam pembayaran elektronik, yang merupakan tindakan ilegal yang dapat merugikan baik pihak perbankan maupun nasabah. Penelitian ini menguraikan penerapan SVM dalam identifikasi kecurangan pada transaksi kartu kredit, dengan fokus pada proses deteksi anomali atau outlier dalam dataset sebagai dasar untuk menetapkan adanya kecurangan dalam transaksi tersebut. Desain sistem ini menunjukkan implementasi metode SVM dalam sistem pendukung pengambilan keputusan (SPPK) untuk institusi perbankan dalam konteks transaksi kartu kredit. Dalam hal ini, SPPK berfungsi sebagai alat verifikasi untuk setiap transaksi yang terjadi. Sistem ini diharapkan dapat membantu pihak perbankan dalam mengidentifikasi indikasi kecurangan yang mungkin muncul, sehingga memungkinkan tindakan cepat diambil, seperti penghentian transaksi atau pemblokiran sementara.

Hasil percobaan pada desain SPPK yang diajukan menunjukkan bahwa sistem ini mampu mengidentifikasi data outlier yang dianggap sebagai indikasi fraud. Hasil tersebut akan digunakan sebagai data yang dikirimkan kepada pihak perbankan sebagai pemberitahuan mengenai kecurangan yang terdeteksi. Jumlah data pelatihan yang masih tergolong sedikit dapat memengaruhi tingkat akurasi dan kecepatan sistem. Oleh karena itu, penelitian selanjutnya diharapkan dapat melaksanakan implementasi pada data nyata di sektor perbankan dengan ukuran data yang lebih besar.

Seiring dengan meningkatnya penggunaan kartu kredit, risiko penipuan yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab juga mengalami peningkatan. Identifikasi transaksi penipuan kartu kredit dapat dilakukan dengan memanfaatkan teknologi pembelajaran ML. Tujuan dari penelitian ini adalah untuk membangun model deteksi transaksi penipuan kartu kredit yang tidak hanya memiliki kinerja yang baik, tetapi juga dapat melakukan proses deteksi dalam waktu komputasi yang singkat, dengan menggunakan metode SVM yang dilengkapi dengan optimasi grid search dan algoritma genetik (genetic algorithm). Terdapat beberapa tantangan utama dalam pengolahan data transaksi antara lain: besarnya dimensi data, ketidakseimbangan kelas, dan kebutuhan akan proses deteksi yang dapat dilakukan dalam waktu komputasi yang singkat. Oleh karena itu, terdapat kebutuhan untuk mengembangkan model dan algoritma optimasi yang tepat guna mengatasi permasalahan tersebut. (Hasibuan & Jannah, 2023).

Hasil penelitian yang dilakukan menunjukkan bahwa dari tiga model yang dikembangkan, model SVM yang memanfaatkan dataset awal yang seimbang dengan teknik Adaptive Synthetic Sampling (ADASYN) serta pencarian parameter optimal melalui *grid search* sebagai metode optimisasi *hyperparameter*, ini mampu melakukan pendeteksian dengan baik serta memiliki waktu komputasi yang relatif singkat. Model ini berhasil mendeteksi transaksi *fraud* dengan sensitivitas sebesar 99% dan spesifisitas sebesar 99%, serta memiliki waktu pelatihan model yang paling efisien dibandingkan dengan kedua model lainnya.

Bentuk penipuan senantiasa mengalami perubahan seiring dengan perkembangan model transaksi. Penelitian (Sarker et al., 2024) melalui penerapan

model *Random Forest* (RF), *Decision Tree* (DT), *Support Vector Machine* (SVM), dan Naïve Bayes. Penelitian ini diharapkan dapat memberikan kontribusi bagi konsumen dan lembaga perbankan dalam memulihkan pendapatan mereka dengan mengembangkan model yang lebih efisien dalam mengidentifikasi transaksi yang bersifat penipuan maupun non-penipuan, menggunakan variabel waktu dan jumlah dari kumpulan data Kaggle. Melalui penerapan beberapa model tersebut diperoleh hasil yang menunjukkan bahwa pengklasifikasi RF memiliki akurasi dan nilai presisi skor f1 yang terbaik. Oleh karena itu, model ini menjadi pilihan yang paling tepat untuk mendeteksi adanya penipuan dalam transaksi.

K-Nearest Neighbour (KNN) merupakan salah satu model algoritma ML yang dapat digunakan untuk mendeteksi fraud dengan cara mengklasifikasikan transaksi berbasis algoritma berbasis lazy learning yang dapat memprediksi dengan menemukan titik data paling dekat dalam klasifikasinya (Tanapanichkan et al., 2024). KNN merupakan algoritma nonparametric, yang berarti tidak ada parameter atau jumlah parameter tetap terlepas dari ukuran data. Sebaliknya parameter akan ditentukan oleh ukuran kumpulan data, meskipun tidak ada asumsi yang perlu dibuat untuk distribusi data yang mendasarinya. pengklasifikasi KNN bergantung pada jarak/ukuran kesamaan yang digunakan (Uddin et al., 2022).

Penggunaan metode KNN dalam klasifikasi *big data* dilakukan dengan k-*means clustering* untuk memisahkan *dataset* menjadi beberapa bagian. Kemudian setiap subset diklasifikasikan dengan metode KNN. kTree dan k*Tree untuk menggunakan jumlah neighbor terdekat yang berbeda untuk klasifikasi KNN. Metode kTree membutuhkan cost operasional yang lebih sedikit tetapi mencapai

akurasi klasifikasi yang serupa dibandingkan dengan metode KNN yang menetapkan nilai K yang berbeda untuk sampel uji yang berbeda. Metode k*Tree adalah perpanjangan dari kTree. Yaitu mempercepat tahap pengujiannya dengan menyimpan informasi sampel pelatihan di leaf node ktree, seperti sampel pelatihan yang terletak di leaf node KNN mereka dan neighbor terdekat dari KNN. Membuat KNN hanya menggunakan subset sampel pelatihan di leaf node. Paper ini menyajikan dua pendekatan yaitu pengklasifikasi direct-cs-knn dan pengklasifikasi distancecs-knn yang bertujuan untuk membuat klasifikasi KNN sensitive terhadap cost sehingga dapat meminimalkan cost kesalahan klasifikasi. Untuk efisiensi beberapa metode yang berguna termasuk smoothing pengaturan K dengan biaya minimum, pemilihan fitur CS dan CS stacking secara signifikan digabungkan ke pengklasifikasi CS-KNN (Zhang, 2020).

Algoritma KNN menyimpan semua data masukan dengan label yang sesuai dan mengklasifikasinya berdasarkan kemiripan dengan tetangga terdekatnya. Algoritma KNN telah digunakan pada beberapa aplikasi kerangka kerja Industri 4.0, seperti keamanan siber, prediksi masa pakai pesawat, klasifikasi kesalahan, prediksi nefropati pada anak-anak, sistem deteksi intrusi. Untuk menentukan titik data mana yang paling dekat dengan pengamatan baru, kita harus mengukur jarak antara titik data. Ada beberapa jenis fungsi yang dapat digunakan untuk memperoleh jarak antara titik, seperti ukuran kesamaan kosinus, Minkowsky, korelasi, Chi-kuadrat, dan jarak Euclidean. Dari semua fungsi tersebut, fungsi yang paling banyak digunakan adalah jarak *Euclidean*, yang merupakan ukuran garis lurus antara dua titik dan untuk dua dimensi (Lopez-Bernal et al., 2021).

Berdasarkan paparan teori sebelumnya *fraud* telah menjadi isu yang sangat penting dalam bidang analisis data dan keamanan finansial yang dapat mengakibatkan kerugian signifikan bagi individu maupun lembaga keuangan. Berdasarkan beberapa paparan hasil penelitian sebelumnya tersebut, sehingga algoritma SVM, RF, K-NN, dan Voting Classifier yang dikenal sebagai salah satu teknik pembelajaran mesin yang efektif, diterapkan untuk menangani masalah ini dengan mendeteksi transaksi yang mencurigakan.

Penelitian ini bertujuan untuk mengevaluasi kinerja ML untuk model SVM, RF, K-NN, dan Voting Classifier dalam mengidentifikasi *fraud* dengan memanfaatkan dataset transaksi yang nyata. Sehingga dapat digunakan untuk menguji dan mengkaji riset yang akan dilaksanakan dalam deteksi *fraud* di BPD Sultra, untuk mempelajari dan menemukan pola *fraud* yang mungkin terjadi sehingga dapat diminimalisasi yang diharapkan dapat memberikan dampak positif bagi perkembangan BPD Sultra dalam pelayanannya terhadap nasabah.

2.2 Keaslian Penelitian

Tabel 2.1. Matriks literatur review dan posisi penelitian
Fraud Detection System Menggunakan SVM, RF, KNN, dengan Voting Classifier pada Automatic Teller Machine

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
1	Credit Card Fraud Detection Using Machine Learning Approach: Application of Machine Learning, Decision Trees, K-Nearest Neighbor, Logistic Regression, Naïve Bayes, Random Forest, Support Vector Machine.	Kanal Bhadresh Soni, Madhuri Chopade, Rahul Vaghela. Applied Information Systems and Management (AISM). 2021	Tujuan dari penelitian ini adalah untuk memprediksi real dan fraud transaction berdasarkan jumlah transaksi dengan menggunakan berbagai pendekatan ML seperti Logistik Regresi, Decision Tree, SVM, Naïve Bayes, Random Forest, dan K-NN.	Berbagai teknik, proses, dan model dibangun dan diimplementasikan untuk memerangi penipuan kartu kredit, dan para peneliti sangat tertarik untuk membangun sistem deteksi penipuan kartu kredit yang akurat. Dengan mengamati perbandingan berbagai pendekatan ML, jelas dari model yang didapatkan bahwa Random Forest memberikan akurasi terbaik sebesar 99,947%, dan bekerja dengan baik dalam setiap aspek, yaitu skor akurasi, skor presisi, dan skor recall.	Kekurangan utama dari penelitian ini adalah dataset imbalanced, interpretabilitas rendah, kurang analisis kesalahan klasifikasi, terbatas pada algoritma tradisional, serta belum diuji pada kondisi nyata dan data modern.	Penelitian ini bagus sebagai benchmark awal, tetapi untuk aplikasi nyata perlu diperluas dengan data lebih beragam, teknik balancing yang lebih canggih, dan model modern seperti deep learning atau hybrid ensembles.
2	Analysis of Machine Learning Classifiers for Speaker Identification: A Study on SVM, Random Forest, KNN, and Decision Tree	Haneen Arafat Gregorius Airlangga. Journal of Computer Networks, Architecture and	Studi ini meneliti kinerja pengklasifikasi ML dalam domain identifikasi pembicara, sebuah komponen penting dari sistem keamanan digital modern. Dengan	Hasil yang dilaporkan bahwa Random Forest (RF) adalah algoritma paling unggul untuk tugas *speaker identification* menggunakan fitur MFCC dari dataset LibriSpeech. RF mencapai hampir sempurna pada semua metrik (precision, recall,	• Penggunaan RF: Disarankan sebagai pilihan utama untuk sistem identifikasi suara karena konsistensi dan akurasinya yang tinggi. • KNN untuk aplikasi real-time: Cocok digunakan pada sistem yang membutuhkan kecepatan	Menunjukkan bahwa ensemble methods (RF) dan distance-based classifiers (KNN) adalah solusi paling efektif untuk speaker identification, sementara SVM dan DT memerlukan optimasi lebih lanjut agar dapat bersaing.

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
		High Performance Computing 2024.	semakin banyaknya integrasi antarmuka yang diaktifkan suara dalam teknologi, permintaan akan identifikasi pembicara yang akurat dan andal sangatlah penting. Penelitian ini memberikan perbandingan komprehensif dari empat pengklasifikasi yang banyak digunakan: Support Vector Machine (SVM), Random Forest (RF), K-Nearest Neighbors (KNN), dan Decision Tree (DT).	F1-score, accuracy ≈ 0.98–0.99), menunjukkan ketahanannya terhadap overfitting dan kemampuannya menangkap pola kompleks suara. KNN juga menunjukkan performa tinggi (≈0.94), cocok untuk aplikasi yang membutuhkan eksekusi cepat dan interpretabilitas. Sebaliknya, SVM hanya mencapai hasil moderat (≈0.80–0.83), menandakan perlunya optimasi lebih lanjut, sementara Decision Tree (DT) memiliki performa paling rendah (≈0.76), rentan terhadap overfitting dan kurang mampu menangkap kompleksitas data.	dan interpretabilitas, misalnya autentikasi suara pada perangkat pintar. • Optimasi SVM: Perlu eksplorasi kernel non-linear dan tuning parameter lebih lanjut agar hasilnya lebih kompetitif. • DT sebaiknya digunakan dengan hati-hati: Karena rentan overfitting, lebih baik dipakai sebagai bagian dari ensemble (misalnya dalam RF) daripada berdiri sendiri. Arah penelitian masa depan: Mengembangkan model hibrida (misalnya menggabungkan RF dengan teknik deep learning) serta menguji performa pada dataset yang lebih bervariasi dan kondisi akustik nyata.	
3	Penggunaan Algoritma Support Vector Machine (SVM) Untuk Deteksi Penipuan pada Transaksi Online	Handry Eldo, Ayuliana, Dikky Suryadi, Giatika Chrisnawati, Loso Judijanto. Jurnal Minfo Polgan. 2024	Mengembangkan model deteksi penipuan menggunakan algoritma Support Vector Machine (SVM). Algoritma SVM dipilih karena kemampuannya dalam mengklasifikasikan data yang kompleks dan	Algoritma SVM dapat dijadikan sebagai solusi yang andal untuk mengidentifikasi penipuan pada transaksi online	Perlu dilakukan pengujian lebih lanjut pada berbagai jenis dataset untuk meningkatkan generalisasi model algoritma yang akan digunakan sebagai perbandingan.	Algoritma di analisis dengan menggunakan model ML SVM yang dibandingkan dengan KNN untuk deteksi kecurangan yang terjadi ketika sedang bertransaksi dengan menggunakan ATM. Hal ini tidak hanya pada transaksi yang terjadi secara online, tetapi juga transaksi yang secara offline.

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
			menangani data dengan dimensi tinggi.			
4	Deteksi Penipuan Kartu Kredit Menggunakan Support Vector Machine dengan Optimasi Grid Search dan Genetic Algorithm	Lailan Sahrina Hasibuan, Fatimah Alfiatul Jannah. Building of Informatics, Technology and Science (BITS). 2023	Membangun model pendeteksian transaksi penipuan kartu kredit yang mampu menghasilkan performa baik serta waktu komputasi singkat menggunakan metode support vector machine (SVM) dengan optimasi grid search dan genetic algorithm.	Dari tiga model yang dibangun, diperoleh bahwa model SVM menggunakan dataset awal yang diseimbangkan dengan ADASYN dan pencarian parameter terbaik dengan grid search sebagai teknik optimasi hyperparameter mampu melakukan pendeteksian dengan baik dan waktu komputasi yang singkat. Model ini mampu mendeteksi transaksi fraud dengan sentitifitas 99% dan spesifisitas 99% serta waktu pelatihan model yang paling singkat diantara dua model lainnya.	Potensi Pengembangan Lebih Lanjut: Meskipun model SVM dengan kernel RBF menunjukkan hasil yang memuaskan, penelitian ini membuka peluang untuk pengembangan lebih lanjut, seperti optimasi parameter menggunakan algoritma lain dan kombinasi dengan teknik machine learning lainnya untuk meningkatkan kinerja deteksi.	Melakukan analisis dan deteksi dengan klasifikasi SVM yang selanjutnya dibandingkan dengan KNN pada dataset langsung real dari lapangan tanpa dilakukan perbandingan dataset tetapi akan digunakan penyeimbangan dataset diawal.
5	Credit Card Fraud Detection Using Machine Learning Techniques	Ananya Sarker, Must. Asma Yasmin, Md. Atikur Rahman, Md. Harun Or Rashid, Bristi Rani Roy, Journal of Computer and Communication, 2024.	Tujuan dari penelitian ini adalah untuk membuat pengklasifikasi *Machine Learning* yang tidak hanya mendeteksi penipuan tetapi juga mendeteksi transaksi yang sah.	Hasil penelitian dengan kumpulan data yang besar dalam penelitian ini dan menggunakan empat ML: Support Vector Machine (SVM), Decision Tree, Naïve Bayes, dan Random Forest. Pengklasifikasi Random Forest mencetak akurasi keseluruhan 99,96% dengan presisi, keingatan, skor f1-, dan	Perlu dilakukan pengujian lebih lanjut pada berbagai jenis dataset untuk meningkatkan generalisasi model dengan penyeimbangan yang baru. Serta dilakukan pengujian dengan data set yang berbeda sumber.	Penelitian ini akan menggunakan dataset dengan jumlah yang besar yang dilakukan penyeimbangan data sebelum dilakukan pengujian klasifikasi dengan SVM dan dibandingkan dengan KNN.

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
				koefisien korelasi Matthews terbaik dalam percobaan.		
6	Comparison and analysis of logistic regression, Naı¨ve Bayes and KNN machine learning algorithms for credit card fraud detection	Fayaz Itoo, Meenakshi, Satwinder Singh. Int. j. inf. tecnol. 2020	Bertujuan untuk mendapatkan hasil pengembangan dari teknik pengambilan sampel ulang (over-sampling atau under-sampling) untuk hasil yang lebih baik dalam deteksi fraud menggunakan tiga algoritma pembelajaran mesin, yaitu: regresi logistik, Naïve Bayes, dan K-nearest neighbor. Kinerja algoritma ini dicatat dengan analisis komparatifnya.	Menyimpulkan bahwa Regresi Logistik (LR) menunjukkan kinerja optimal untuk semua proporsi data dibandingkan dengan NB dan KNN. LR memiliki akurasi yang lebih tinggi dibandingkan dengan NB dan KNN. Dengan akurasi maksimum masing-masing 95%, 91%, dan 75%. Teknik LR juga menunjukkan Sensitivitas, Spesifisitas, Presisi, dan F-Measure yang lebih baik dibandingkan dengan teknik NB dan K-NN.	Keterbatasan utama Random Undersampling adalah beberapa informasi dapat hilang dan metode resampling baru dapat dirancang untuk mencapai hasil optimal yang dapat terbukti membantu dalam deteksi penipuan kartu kredit (CCFD) di masa mendatang.	Analisa kecurangan dengan kartu kredit sudah banyak dilakukan, akan tetapi transaksi dengan ATM belum banyak dilakukan. Termasuk dalam penggunaan ML, klasifikasi SVM dan KNN yang akan dikembangkan dengan pra sampling pada sampel yang akan digunakan sebelum dilakukan analisis.
7	Credit card fraud detection using artificial neural network	Asha RB, Suresh Kumar KR, Global Transitions Proceedings, 2021.	Untuk memenuhi kebutuhan, kartu kredit digunakan dan penipuan yang terkait dengannya juga meningkat, sehingga ada kebutuhan untuk mengembangkan model yang cocok dan memprediksi dengan akurasi yang lebih tinggi.	Dengan menggunakan artificial neural network (ANN) yang memberikan akurasi kira-kira sama dengan 100% paling cocok untuk deteksi penipuan kartu kredit. Ini memberikan akurasi lebih dari algoritma pembelajaran tanpa pengawasan.	Perlu dilakukan penelitian, pra-pemrosesan data, normalisasi dan under-sampling dilakukan untuk mengatasi masalah yang dihadapi dengan menggunakan dataset yang tidak seimbang untuk mengetahui pengaruh masing-masing klasifikasi ML untuk model yang lain.	Penelitian ini akan menggunakan klasifikasi SVM dan KNN untuk deteksi kecurangan transaksi yang terjadi pada ATM.

2.3 Landasan Teori

a. *Machine Learning*

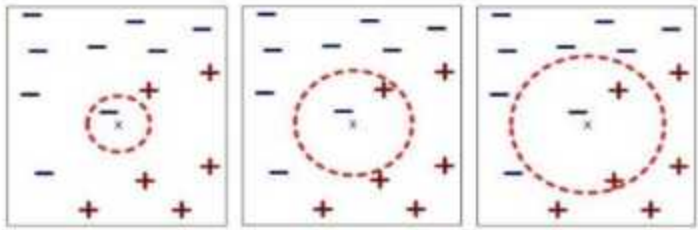
Machine learning (ML) merupakan suatu bidang dalam kecerdasan buatan (AI) yang memungkinkan sistem komputer untuk belajar dan berkembang secara mandiri. Metode ini memanfaatkan data dan algoritma guna memungkinkan sistem komputer meniru cara pembelajaran manusia. Machine learning, yang juga dikenal dengan istilah pembelajaran mesin, adalah cabang ilmu komputer yang beroperasi tanpa memerlukan pemrograman eksplisit. Banyak peneliti berupaya untuk membuat kemajuan menuju kecerdasan buatan yang setara dengan kemampuan manusia. Machine learning ini juga berfungsi sebagai kecerdasan buatan yang mempelajari cara menghasilkan data. Singkatan umum untuk machine learning adalah ML. Bidang ini menjadi sangat penting untuk penerapan teknik yang cepat dan efektif dalam mengidentifikasi dan menyelesaikan masalah baru (Dinata & Hasdina, 2020).

Secara definisi, ML adalah ilmu yang mengeksplorasi algoritma dan model statistik yang digunakan oleh sistem komputer untuk menjalankan tugas tertentu tanpa instruksi yang jelas. Machine learning mengandalkan pola dan kesimpulan. Untuk memperoleh pola dan kesimpulan tersebut, algoritma machine learning menciptakan model matematis yang berbasis pada data sampel yang kerap disebut dengan training data. Penggunaan teknik ini terkait dengan pembelajaran mesin dan AI. Mesin ini membuktikan kepada algoritma atau program yang beroperasi di komputer. Segala pengetahuan machine learning akan melibatkan data.

b. K-Nearest Neighbors

K-Nearest Neighbor (KNN) menunjukkan kinerja yang memuaskan dalam klasifikasi ketika diterapkan pada dataset dengan ukuran kecil. Metode ini melakukan evaluasi terhadap kesamaan dari catatan pelatihan yang paling dekat. Nilai \(k \) merujuk pada jumlah tetangga yang dianalisis, yang menggambarkan seberapa banyak data terdekat yang dievaluasi dalam proses klasifikasi (Purwaningsih & Nurelasari, 2021). KNN merupakan algoritma Machine Learning yang bersifat non-parametrik dan *lazy learning*. Metode non-parametrik menunjukkan bahwa pendekatan tersebut tidak memiliki asumsi tertentu terhadap distribusi data yang mendasarinya. Dengan demikian, tidak terdapat sejumlah parameter atau estimasi parameter yang tetap dalam model, baik pada dataset berukuran kecil maupun besar. Selain itu, algoritma KNN juga tergolong dalam kategori pembelajaran malas (lazy learning), yang berarti bahwa algoritma ini tidak memanfaatkan titik data pelatihan untuk membangun model.

Algoritma seperti KNN mengandalkan sejumlah parameter yang fleksibel, dan jumlah parameter tersebut cenderung meningkat seiring dengan bertambahnya jumlah data. Algoritma non-parametrik, meskipun secara komputasi lebih lambat, cenderung membuat asumsi yang lebih sedikit mengenai data. Dengan demikian, dapat disimpulkan bahwa pada algoritma KNN tidak terdapat fase pelatihan yang signifikan, bahkan jika ada, fase tersebut cenderung sangat terbatas. Metode KNN menggunakan prinsip ketetanggaan (*neighbor*) untuk memprediksi kelas yang baru. Jumlah tetangga yang dipakai adalah sebanyak ktetangga. Prinsip ketetanggaan dapat diilustrasikan pada **Gambar 2.1** berikut:



Gambar 2.1. Ilustrasi *k-Nearest Neighbor*

Setelah mengambil k tetangga terdekat pertama kemudian dihitung jumlah data yang mengikuti kelas yang ada dari k tetangga tersebut. Kelas dengan data terbanyak yang mengikutinya menjadi kelas pemenang yang diberikan sebagai label kelas pada data X. Pada KNN, nilai k dapat memberikan pengaruh terhadap performa klasifikasi yang dihasilkan. Jika nilai k terlalu kecil (Siringoringo, 2018).

Prinsip kerja KNN adalah melakukan klasifikasi berdasarkan kedekatan lokasi (jarak) suatu data dengan data yang lain. Dekat atau jauhnya lokasi (jarak) bisa dihitung melalui salah satu dari besaran jarak yang telah ditentukan yakni jarak Euclidean dan jarak Minkowski, Namun dalam penerapannya seringkali digunakan jarak Euclidean karena memiliki tingkat akurasi dan juga productivity yang tinggi. Jarak Euclidean adalah besarnya jarak suatu garis lurus yang menghubungkan antar objek (Itoo et al., 2021). Berikut tahapan untuk menjalankan proses KNN:

- Menentukan jumlah pada tetangga k
- Menghitung jarak objek dengan masing-masing data kelompok. Perhitungan jarak menggunakan rumus Euclidian distance berikut pada **persamaan 1**:

$$d\,(x_i, y_j)\sqrt{\sum_{n=1}^{p}(x_{ip} - x_{jp})^2} \qquad (1)$$

Ket:
x_{ip} = data testing ke-i pada variabel ke-p
x_{jp} = data training ke-j pada variabel ke-p
$d(x_i, x_j)$ = jarak Euclidean
p = dimensi data variabel bebas

- Didapatkan hasil pengklasifikasian

Adapun Algoritma pengerjaan metode KNN adalah sebagai berikut:

1. Tentukan parameter K (banyak tetangga terdekat)
2. Hitung jarak data baru/data testing dengan semua data yang ada di data training menggunakan persamaan 1
3. Urutkan jarak dan tentukan tetangga mana yang paling dekat berdasarkan jarak minimum ke-K
4. Menentukan kategori dari tetangga terdekat
5. Menggunakan kategori mayoritas yang sederhana dari tetangga terdekat sebagai nilai prediksi data baru.

c. *Support Vektor Machine* (SVM)

Metode klasifikasi yang memaksimalkan batas hyperplane (hyperplane margin maksimal) merupakan komponen krusial dari Support Vector Machine (SVM). Data yang dipilih akan berkontribusi dalam pembentukan model yang digunakan dalam klasifikasi pada penelitian ini. Metode SVM adalah suatu sistem pembelajaran yang menggunakan algoritma yang didasarkan pada prinsip optimasi (Sudin et al., 2023). Konsep SVM melibatkan pencarian hyperplane optimal yang berfungsi sebagai pemisah antara dua kelas. SVM menentukan hyperplane ini berdasarkan data support vector yang terletak paling dekat dengan hyperplane tersebut, sedangkan margin menunjukkan lebar dari hyperplane pemisah. Data yang

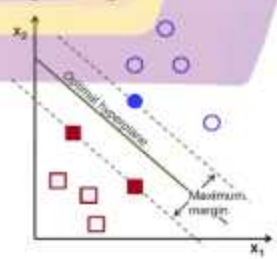
dapat dipisahkan secara linier adalah data yang dapat dibedakan melalui pendekatan linier. Sebagai contoh, misalkan {x1, …, xn} merupakan suatu dataset dan y 1 ∈ {+1, -1} adalah label kelas, di mana data xi yang dilabeli +1 menunjukkan bahwa data tersebut dikategorikan ke dalam kelas +1, sedangkan label -1 menunjukkan sebaliknya. Langkah awal dalam algoritma SVM adalah mendefinisikan persamaan untuk hyperlane pemisah yang dinyatakan dalam **persamaan 2**.

$$W.X + b = 0 \qquad (2)$$

W merupakan sebuah bobot vektor yang dinyatakan sebagai W = {W1, W2, …, Wn}, di mana n adalah jumlah atribut, dan b adalah sebuah skalar yang disebut sebagai bias. Mengacu pada atribut A1 dan A2, dengan asumsi tupel pelatihan X = (x1, x2), di mana x1 dan x2 merupakan nilai dari atribut A1 dan A2, dan dengan mempertimbangkan b sebagai suatu bobot yang ditambahkan (w0), persamaan suatu hyperplane pemisah dapat direpresentasikan dalam **persamaan 3**.

$$w0 + w1x1 + w2x2 = 0 \qquad (3)$$

Setelah persamaan dapat di defenisikan, nilai x1 dan x2 dapat dimasukkan ke dalam persamaan untuk mencari bobot w1, w2, dan w0 atau b, dapat dilihat dari **Gambar 2.2** pemisahan dua kelas data dengan margin maksimum.



Gambar 2.2. Pemisahan dua kelas data dengan margin maksimum (Sudin et al., 2023).

Gambar 2.2 menunjukkan bagaimana SVM menentukan *hyperplane* pemisah maksimum, yang memiliki jarak maksimum antara tupel pelatihan terdekat. Support vector ditandai dengan garis tebal yang mengelilingi titik-titik tupel. Oleh karena itu, setiap titik yang terletak di atas hyperplane pemisah memenuhi **persamaan 4** sebagai berikut:

$$w0 + w1x1 + w1x1 > 0 \quad (4)$$

Sedangkan, titik yang terletak dibawah hyperlane pemisah memenuhi **persamaan 5** berikut:

$$w0 + w1x1 + w1x1 < 0 \quad (5)$$

sehingga, maka diperoleh dua persamaan hyperlane pada **persamaan 6** dan **7** berikut:

$$w1x1 + w1x1 \geq 1 \text{ untuk } yi = +1 \quad (6)$$

$$w1x1 + w1x1 \leq 1 \text{ untuk } yi = -1 \quad (7)$$

dimana:

Xi = data ke -1

W = nilai bobot support vector yang tegak lurus dengan *hyperlane*

b = nilai bobot

yi = kelas data ke – i.

Berdasarkan persamaan tersebut, peneliti menetapkan nilai parameter ambang batas untuk memperoleh hasil prediksi, yaitu ambang batasnya 1. Apabila hasil penjumlahan lebih dari atau sama dengan 1, maka dibaca "Ya". Namun, jika hasilnya kurang dari 1, maka hasilnya "Tidak".

d. *Random Forest (RF)*

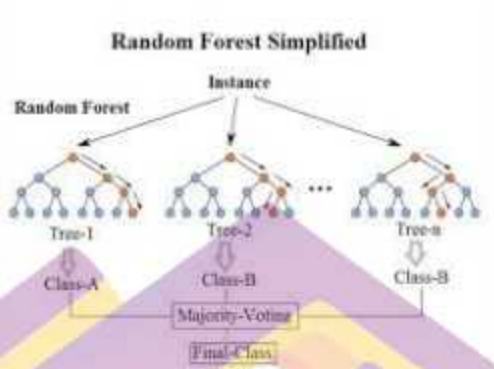
RF merupakan salah satu metode yang dapat meningkatkan hasil akurasi dalam membangkitkan atribut untuk setiap node yang dilakukan secara acak. RF terdiri dari sekumpulan decision tree, dimana kumpulan pohon keputusan ini digunakan untuk mengklasifikasi data ke suatu kelas. Pohon keputusan dibuat dengan menentukan node akar dan berakhir dengan beberapa node daun untuk mendapatkan hasil akhir untuk model pohon keputusan yang akurat, namun teknik ini juga dapat menghasilkan model yang kompleks dan sulit diinterpretasikan (Suci Amaliah et al., 2022). Metode RF menghasilkan sejumlah pohon acak, dan kelas yang dihasilkan terbentuk melalui proses klasifikasi yang dipilih dari kelas yang paling umum (modus) yang dihasilkan oleh pohon keputusan yang telah ada.

Membentuk pohon keputusan pada metode RF sama dengan proses pada *Classsification and Regression Tree* (CART), hanya saja pada RF tidak dilakukan *prunning* (pemangkasan). Indeks Gini digunakan untuk memilih fitur di setiap simpul internal dari pohon keputusan. Nilai Indeks Gini dapat dihitung seperti pada **persamaan 8** berikut:

$$Gini(D) = 1 - (p_1^2 + p_2^1) \qquad (8)$$

Dimana, P adalah probabilitas dari kelas 1 dan kelas 2 dalam dataset D.

Selanjutnya dapat dilihat pada **Gambar 2.3** berikut untuk representatif dari model RF yang digunakan.



Gambar 2.3. Model Random Forest

e. *Ensemble Voting Classifier*

Ensemble voting classifier merupakan suatu pendekatan pembelajaran mesin yang mengintegrasikan beberapa model pembelajaran untuk meningkatkan kinerja prediksi. Konsep ini melibatkan penggunaan beberapa algoritma pembelajaran untuk membangun sejumlah model independen, yang kemudian digabungkan bersama untuk menghasilkan prediksi akhir. Dalam proses ensemble voting classifier , setiap model memberikan suara atau kontribusi berdasarkan prediksi yang dibuatnya. Suara dari setiap model kemudian dijumlahkan atau diambil rata-rata dan kelas yang mendapat suara terbanyak dipilih sebagai prediksi akhir (Dede Kurniadi et al., 2025).

Ensemble voting dalam metode yang akan digunakan adalah menggabungkan beberapa algoritma klasifikasi berbeda, RF, SVM, dan KNN dengan cara melakukan pemungutan suara terhadap hasil prediksi masing-masing model untuk menghasilkan keputusan akhir yang lebih akurat dan stabil. Pada skema *hard voting*, kelas akhir dipilih berdasarkan mayoritas label yang diprediksi

ketiga model, sedangkan pada skema *soft voting* kelas akhir ditentukan berdasarkan rata-rata (atau rata-rata berbobot) probabilitas kelas dari ketiga model tersebut (Jauhari et al., 2024). Ensemble voting classifier dibagi menjadi dua jenis yaitu hard voting dan soft voting. Berikut penjelasannya masing-masing.

1. Hard voting classifier adalah teknik ensemble pada klasifikasi di mana beberapa model (*base learnerx*) memberikan prediksi kelas, lalu kelas akhir dipilih berdasarkan suara mayoritas (*majority vote*). Teknik ini sering dipakai ketika tiap model memberi label kelas (bukan probabilitas) dan tujuannya adalah memperkuat keputusan dengan menggabungkan beberapa model sekaligus (Fauzi & Bours, 2020). Hard voting memilih kelas yang paling sering muncul di antara $\{h_1(x), \ldots, h_M(x)\}$. Secara sederhana: "tiap model 1 suara, kelas dengan suara terbanyak menang". Jika terjadi seri, biasanya dipecahkan dengan aturan tambahan, misalnya memilih kelas dengan prioritas tertentu atau menggunakan probabilitas (jika tersedia) sebagai tiebreaker. Aturan keputusan hard voting untuk kelas k pada **Persamaan 9** berikut:

$$\hat{y}(x) = \arg\max_{k} \sum_{j=1}^{M} I\left(h_j(x) = k\right) \qquad (9)$$

di mana:

- $\hat{y}(x)$ adalah kelas prediksi akhir untuk sampel x.
- k adalah salah satu kelas dalam himpunan kelas (misalnya {0,1} untuk fraud / not fraud).
- $I(\cdot)$ adalah fungsi indikator: bernilai 1 jika pernyataan benar, 0 jika salah.

Makna rumus: untuk setiap kelas k, hitung berapa banyak model yang memprediksi kelas k, lalu pilih kelas dengan jumlah terbanyak. Jika menggunakan bobot pada tiap model (*weighted hard voting*), rumusnya bisa ditulis seperti pada **Persamaan 10** berikut:

$$\hat{y}(x) = \arg\max_{k} \sum_{j=1}^{M} w_j \, I(h_j(x) = k) \quad (10)$$

dengan w_j bobot/importance model ke-j, untuk model bagan dari hard voting ditunjukkan pada **Gambar 2.4** berikut ini.

Gambar 2.4. Model Hard Voting Classifier

2. Soft Voting Classifier, merupakan metode ensemble learning dalam machine learning di mana prediksi akhir dihasilkan dengan merata-ratakan probabilitas kelas dari setiap model dasar (base classifier), kemudian memilih kelas dengan probabilitas rata-rata tertinggi. Berbeda dengan hard voting yang hanya menggunakan majority vote berdasarkan label kelas, soft voting memanfaatkan estimasi probabilitas untuk memberikan bobot lebih pada prediksi yang lebih yakin (Sherazi et al., 2021).

Dengan kelebihan yang akurat daripada hard voting karena mempertimbangkan tingkat keyakinan (confidence) model, mengurangi bias dan varians, serta meningkatkan performa pada dataset kompleks.

Akan tetapi dibalik kelebihan tersebut, adapun kekurangannya yaitu memerlukan model dasar yang mendukung estimasi probabilitas (seperti dengan probability=True pada SVM), komputasi lebih tinggi, dan bergantung pada keragaman model untuk efektivitas (Cao-Van et al., 2024). Setiap model tidak hanya mengeluarkan label kelas, tetapi juga estimasi probabilitas keanggotaan kelas. Jika bobot sama, rumus di atas ekuivalen dengan memilih kelas dengan rata-rata probabilitas terbesar.

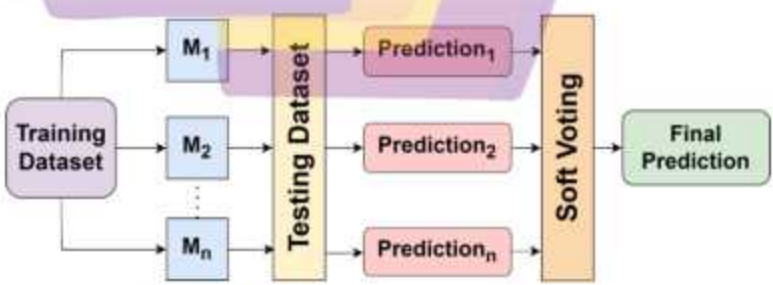
Aturan keputusannya seperti **Persamaan 11** berikut:

$$\hat{y}(x) = \arg\max_{k \in K} \sum_{j=1}^{M} w_j \, p_j(k \mid x) \qquad \text{(Per.11)}$$

dengan:

- $p_j(k \mid x)$: probabilitas yang diprediksi model ke-j bahwa sampel x termasuk kelas k,
- w_j: bobot model ke-j (umumnya $w_j = 1$ untuk unweighted soft voting).

Berikut untuk model bagan dari soft voting ditunjukkan pada **Gambar 2.5** berikut ini.



Gambar 2.5. Model Hard Voting Classifier

BAB 3

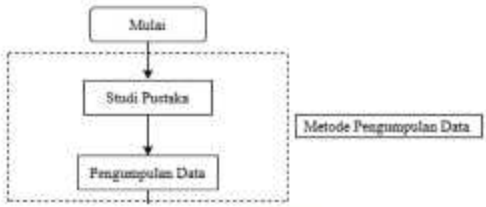
METODE PENELITIAN

3.1 Jenis, Sifat dan Pendekatan Penelitian

Penelitian ini merupakan penelitian kuantitatif dengan sifat deskriptif dan eksploratif. Dimulai dari identifikasi permasalahan utama dalam kecurangan transaksi ATM secara online dan offline, dilakukan studi literatur untuk memahami kekuatan dan kelemahan metode SVM, RF, K-NN dengan *Voting Classifier* dalam analisis kecurangan dalam transaksi dengan ATM serta mengkaji penelitian yang relevan untuk memastikan penelitian ini berkontribusi pada pengembangan pengetahuan. Tahapan selanjutnya dilakukan pendekatan dengan pengumpulan data primer melalui eksperimen interaksi pengguna sedangkan dengan data sekunder dari dataset transaksi ATM yang mengalami *fraud*. Penggunaan dataset dari ATM merupakan novelty dari penelitian yang dikaji. Hal ini berdasarkan data penelitian sebelumnya yang telah dipaparkan, deteksi yang dilakukan adalah melalui *credit card* dan transaksi online.

3.2 Metode Pengumpulan Data

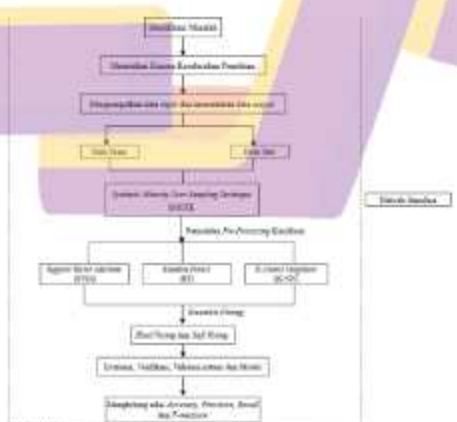
Untuk mengklasfikasi deteksi kecurangan pada transaksi menggunakan ATM baik online maupun offline ada beberapa pendekatan penelitian menggunakan metode kuantitatif, lalu pada tahap metode penelitian yang akan dilakukan adalah pengumpulan data dengan fitur terkait, pengolahan data awal (pre-processing data), lalu melakukan penerapan dengan algoritma SVM, RF, K-NN, dan *Voting Classifier* pada dataset. Metode ini terdiri dalam beberapa tahapan sekaligus seperti yang ditunjukkan pada **Gambar 3.1** berikut.



Gambar 3.1. Tahap pengumpulan data untuk penelitian

3.3 Metode Analisis Data

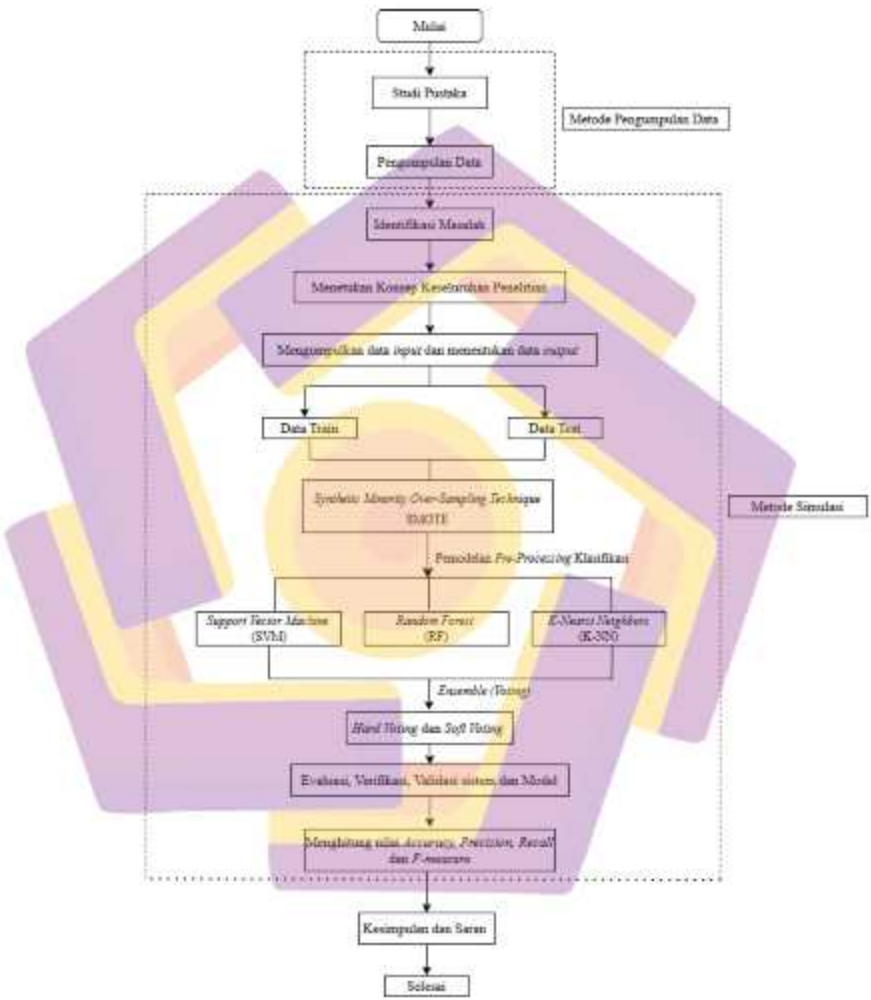
Pengolahan Data dimulai dari identifikasi dataset yaitu memiliki tipe data, data *redundant* dan *null* data. Setelah melakukan analisa data, tahap selanjutnya melakukan *pre-processing*, kemudian melakukan split dataset yaitu pembagian data training dan data testing yang akan dianalisis. Hasil analisis selanjutnya dilakukan perhitungan nilai hasil analisis dengan menggunakan *confusion matrix* (Maulani & Sari, 2023). Dalam metode ini dilakukan beberapa tahapan untuk analisis dan interpretasi data dari hasil analisis yang dilakukan seperti yang ditunjukkan pada **Gambar 3.2** berikut.



Gambar 3.2. Keseluruhan metode analisis dan interpretasi termasuk metode simulasi

3.4 Alur Penelitian

Alur penelitian secara umum disajikan seperti pada **Gambar 3.3** berikut ini.



Gambar 3.3. Alur penelitian secara umum

BAB 4

HASIL PENELITIAN DAN PEMBAHASAN

4.1 Pengumpulan Data

Pengumpulan data dilakukan dengan observasi secara langsung dengan akses *database* pada BPD Bank Sultra yang telah diberikan ijin penelitian dengan nomor 016/DAAK/AMIKOM/V/2025. Kumpulan data yang digunakan merupakan data transaksi ATM pada periode bulan September 2025 sejumlah 200.521 record transaksi ATM yang mencakup 24 fitur, salah satu karakteristik penting dari dataset ini adanya ketidakseimbangan kelas (*class imbalance*) yang signifikan dengan transaksi non fraud sebanyak 188.730 record (94%) dan transaksi *fraud* 11.791 record (5,88%). Dataset memiliki variasi tipe data yang terdiri dari data numerik antara lain no_kartu, no_rek,kd_cab_rek,kode_tx,jam_tx, rcode, jumlah_tx, kd_bank_tujuan, saldo_akhir, no_rek_penerima. Data kategorial 7 kolom antara lain terminal, no_arsip, keterangan, nama_singkat, tgl_tx, time_stamp.

Dataset transaksi ATM Bank Sultra terdiri dari 24 fitur yang merepresentasikan berbagai aspek dari setiap transaksi yang terjadi. Fitur-fitur tersebut dapat dikelompokkan ke dalam lima kategori besar, yaitu identitas kartu dan rekening, informasi terminal dan kode bank, detail transaksi, informasi rekening tujuan, serta label kelas fraud. Kelompok pertama adalah fitur identitas kartu dan rekening, yang terdiri dari tiga kolom. NO_KARTU merupakan nomor kartu ATM yang digunakan nasabah untuk melakukan transaksi; fitur ini bersifat unik per kartu dan menjadi penanda identitas utama nasabah. NO_REK adalah

nomor rekening yang terhubung dengan kartu ATM tersebut, yang menghubungkan transaksi dengan akun pemilik secara langsung. KD_CAB_REK merupakan kode cabang tempat rekening nasabah terdaftar, yang dapat digunakan untuk mengidentifikasi apakah transaksi dilakukan di luar cabang asal nasabah. OPENDATE adalah tanggal pembukaan sistem pada perbankan rekening dalam format numerik (DDMMYYYY), yang dapat memberi informasi tanggal transaksi yang terjadi.

Kelompok kedua adalah fitur terminal dan kode bank, yang mencakup informasi infrastruktur dan lokasi transaksi. TERMINAL adalah kode identitas mesin ATM yang digunakan dalam transaksi, berfungsi untuk mengidentifikasi lokasi fisik ATM. KD_BANK_LOKTX adalah kode bank yang mengoperasikan ATM tempat transaksi dilakukan, sedangkan KD_BANK_LOKREK adalah kode bank pemilik rekening nasabah. Kombinasi dari dua fitur ini memungkinkan identifikasi apakah transaksi terjadi di jaringan bank sendiri atau jaringan bank lain (transaksi interbank). KD_BANK_TUJUAN adalah kode bank tujuan untuk transaksi transfer antar bank, di mana nilai null mengindikasikan transaksi non-transfer seperti tarik tunai atau cek saldo. Fitur ini memiliki missing values yang tinggi (52,42%) karena tidak semua transaksi melibatkan transfer ke bank lain, sehingga kondisi ini adalah wajar.

Kelompok ketiga adalah fitur detail transaksi, yang merupakan kelompok terbesar dan paling informatif. KODE_TX adalah kode numerik yang merepresentasikan jenis transaksi yang dilakukan, seperti tarik tunai, transfer, cek saldo, dan sebagainya. JENISTX adalah fitur kategorikal yang mendeskripsikan

jenis transaksi secara lebih eksplisit. JUMLAH_TX merupakan nominal jumlah uang yang ditransaksikan dalam satuan rupiah, menjadi salah satu fitur numerik utama karena pola jumlah transaksi yang besar secara tiba-tiba merupakan sinyal kuat potensi fraud. RCODE adalah response code yang menunjukkan hasil dari transaksi, di mana kode 00 berarti transaksi berhasil, kode 51 berarti saldo tidak mencukupi, dan kode lainnya mengindikasikan berbagai kondisi kegagalan sistem. FLAG_TX merupakan binary flag yang menandai status transaksi, di mana nilai 0 menunjukkan transaksi normal dan nilai 1 menunjukkan transaksi dengan status reversal (pembatalan transaksi akibat timeout atau kegagalan sistem). NO_ARSIP adalah nomor arsip unik untuk setiap transaksi yang berfungsi sebagai referensi rekam jejak transaksi dalam sistem. JAM_TX adalah waktu transaksi dalam format HHMMSS (jam, menit, detik), yang sangat krusial sebagai indikator fraud karena pelaku fraud cenderung beroperasi di luar jam operasional, khususnya pada tengah malam hingga dini hari. TGL_TX adalah tanggal transaksi dalam format standar, sedangkan TIME_STAMP adalah timestamp presisi tinggi yang merekam waktu transaksi hingga level milidetik termasuk zona waktu, sangat berguna untuk mendeteksi transaksi beruntun (sequential transactions) dalam waktu yang sangat berdekatan. KETERANGAN adalah deskripsi transaksi yang biasanya berisi kode referensi atau keterangan singkat mengenai jenis transaksi yang dilakukan. KET_LAIN2 adalah keterangan tambahan yang berisi informasi pelengkap transaksi, seperti pesan konfirmasi "TRANSAKSI BERHASIL!" atau keterangan lainnya.

Kelompok keempat adalah fitur informasi rekening tujuan, yang relevan khususnya untuk transaksi transfer. SALDO_AKHIR adalah saldo rekening nasabah setelah transaksi dilakukan dalam satuan rupiah; rasio antara jumlah transaksi dan saldo akhir dapat menjadi indikator fraud apabila nilainya mendekati habis secara signifikan. NO_REK_PENERIMA adalah nomor rekening tujuan transfer, yang memiliki missing values sangat tinggi (65,80%) karena hanya terisi untuk transaksi yang memiliki rekening penerima. KD_CAB_REK_PENERIMA adalah kode cabang bank penerima transfer, yang bersama KD_BANK_TUJUAN membentuk informasi lengkap mengenai tujuan aliran dana. NAMA_SINGKAT adalah nama singkat pemilik rekening tujuan, yang juga memiliki missing values tinggi (60,47%) karena hanya tersedia untuk transaksi transfer antar rekening.

Kelompok kelima adalah fitur label kelas, yaitu IS_FRAUD yang merupakan variabel target (target variable) dalam penelitian ini. Fitur ini bersifat biner dengan nilai 1 menandakan transaksi teridentifikasi sebagai fraud dan nilai 0 menandakan transaksi yang sah (legitimate). Dari total 200.521 record, sebanyak 188.730 transaksi (94,12%) berlabel non-fraud dan 11.791 transaksi (5,88%) berlabel fraud, mencerminkan kondisi class imbalance yang signifikan dengan rasio 1:16 yang menjadi tantangan utama dalam pemodelan machine learning pada penelitian ini.

4.2 Pre-Processing, Training dan Testing Dataset

Pada tahap ini peneliti melakukan preprocessing dataset menggunakan Google Collab dengan python 3.10 beserta core library yang digunakan Pandas versi 2.2.2 berfungsi untuk manipulasi dan analisis data dalam bentuk DataFrame,

Numpy versi 2.0.2 digunakan untuk operasi numerik dan array multidimensi, Matplotlib & Seaborn digunakan untuk visualisasi data dan hasil analisis. Dalam tahapan ini, dilakukan langkah pre-processing, training dan testing dataset.

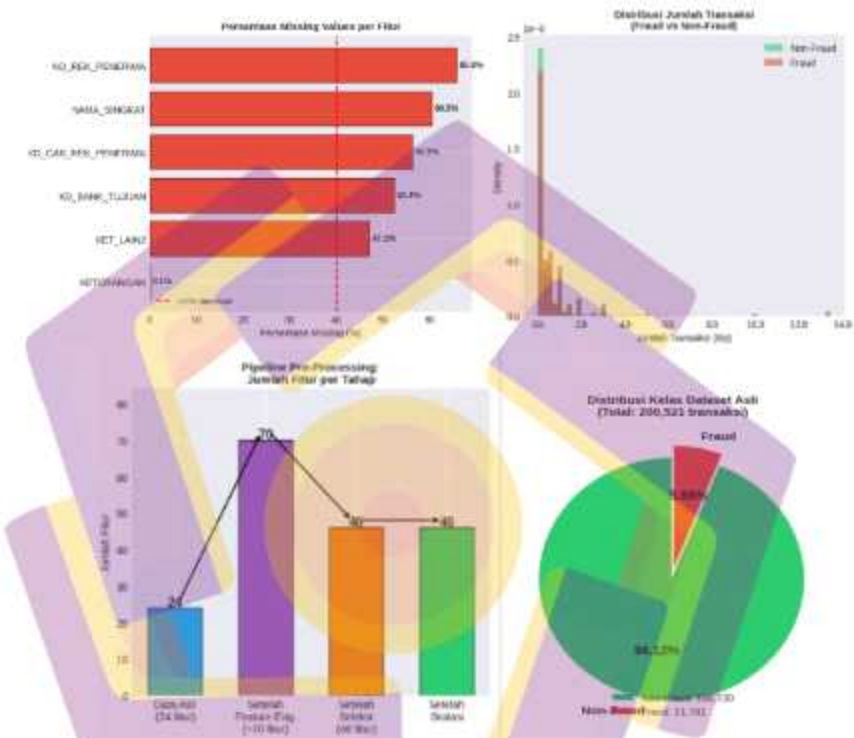
Peneliti memulai dengan Explanatory Data Analysis (EDA) pada tahap ini peneliti mengekstraksi informasi dataset seperti analisis missing values pada dataset transaksi ATM Bank Sultra, hasil explanatory Data Analysis menunjukkan bahwa terdapat beberapa kolom dengan nilai yang hilang dalam jumlah yang bervariasi seperti ditampilkan pada **Tabel 4.1.** berikut.

Tabel 4.1 Tabel Missing Data Pada Dataset

Fitur	Jumlah Missing	Presentase
no_rek_penerima	131.944	65,80%
nama_singkat	121.263	60,47%
kd_cab_rek_penerima	112.797	56,25%
kd_bank_tujuan	105.123	52,42%
ket_lain	94.502	47,13%
keterangan	109	0,05%

Missing values dengan presentase tinggi > 40% pada kolom seperti no_rek_penerima, nama_singkat dan kd_cab_rek_penerima merupakan kondisi yang wajar karena tidak semua transaksi melibatkan transfer rekening ke bank lain seperti transaksi tarik tunai ataupun cek saldo. Penanganan missing values ini dilakukan melalui teknik imputasi yang sesuai dengan jenis dan karakteristik data pada setiap kolom. Pemahaman pola missing values ini penting untuk menentukan strategi penanganan yang tepat tanpa membuang informasi berharga atau membuat

biasa dalam data. Selanjutnya dalam tahap pre-processing data ini dihasilkan visualisasi seperti pada **Gambar 4.1** berikut.



Gambar 4.1. Hasil tahap pre-processing data

Berdasarkan hasil diatas menunjukkan bahwa, analisis missing value dengan Fitur missing values tinggi: NO_REK_PENERIMA (65.8%), NAMA_SINGKAT (60.5%), KD_CAB_REK_PENERIMA (56.3%), KD_BANK_TUJUAN (52.4%), KET_LAIN2 (47.1%); Fitur keterangan tidak memiliki missing values; dengan implikasi missing values yang tinggi dapat menurunkan kualitas model. Oleh karena itu dilakukan imputasi per kolom sehingga setelah tahap ini tidak ada missing values. Dengan distribusi kelas sebagai

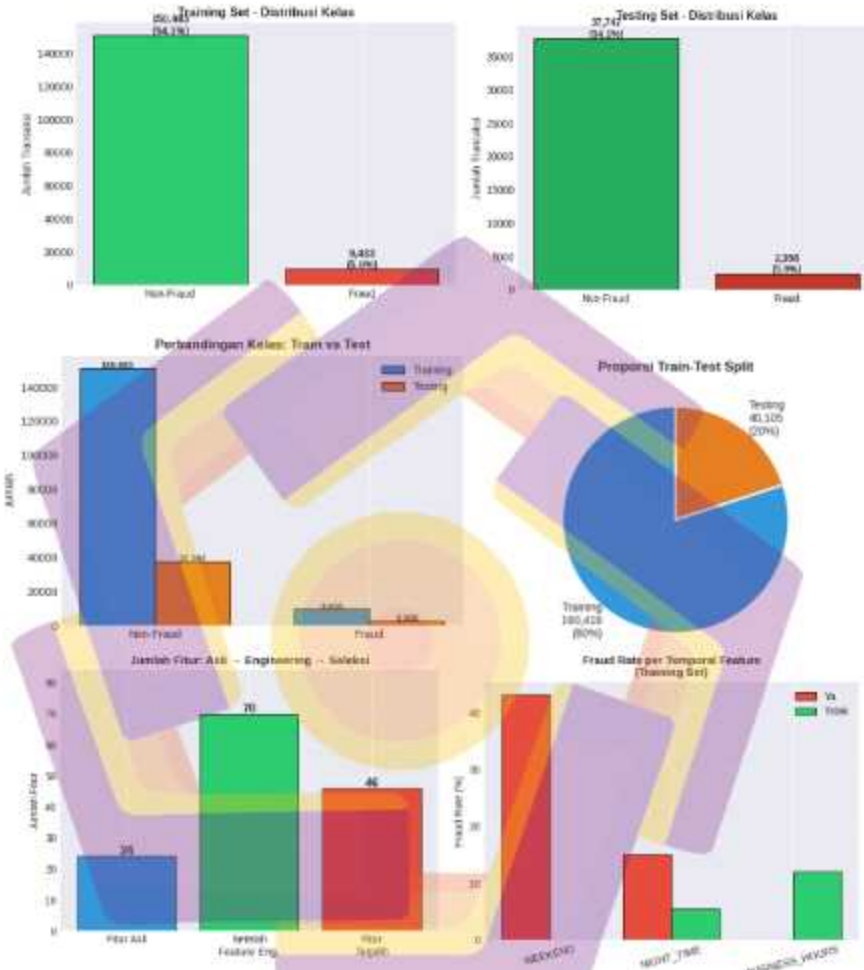
berikut: Non-Fraud: 94.12% (188,730 transaksi); Fraud: 5.88% (11,791 transaksi); Implikasi: Dataset sangat tidak seimbang (class imbalance), model cenderung bias ke kelas mayoritas. Sehingga diperlukan SMOTE pada data training untuk menyeimbangkan rasio kelas menjadi 1:1. sedangkan untuk per-hari *Fraud* sangat tinggi pada hari Minggu (~40%), sementara hari kerja hampir 0%. Hal ini menunjukkan bahwa adanya pola temporal yang signifikan. Untuk feature Engineering dari 24 fitur asli selanjutnya dikembangkan menjadi ~70 fitur dengan tambahan: Temporal markers (jam, hari, akhir pekan), amount-based markers (rasio jumlah transaksi terhadap saldo), behavior markers (frekuensi transaksi, pola penerima). Dari 70 fitur yang dipilih 46 fitur numerik yang relevan dengan seleksi dilakukan untuk mengurangi noise dan overfitting, semua fitur numerik distandarisasi (mean = 0, std = 1) hal ini bertujuan untuk memastikan algoritma berbasis jarak (misalnya KNN, SVM) bekerja optimal. Sehingga dari Pre-Processing model ML untuk fraud detection ini memiliki fondasi yang kuat.

Hasil EDA juga menunjukkan bahwa dataset mengalami *severe class imbalance* dengan rasio 1:16 antara kelas fraud dan non-fraud. Dengan distribusi Kelas 0 (Non Fraud) sebanyak 188.730 transaksi (94.12%) dan kelas 1 (Fraud) sebanyak 11.791 transaksi (5,88%), distribusi ini dapat diliat pada **Gambar 4.2**. berikut. Ini merupakan karakteristik yang umum dalam kasus fraud detection di dunia nyata. Dampak dari imbalance adalah model cenderung bias terhadap kelas mayoritas (non-fraud), akurasi tidak lagi menjadi metrik yang reliable untuk pengukuran, diperlukan teknik khusus untuk menyeimbangkan distribusi kelas

fraud dan non-fraud pada kasus ini peneliti menggunakan SMOTE. Metrik evaluasi pada penelitian harus fokus pada Recall dan F1-Score.

Gambar 4.2. Gambar Distribusi Transaksi Dataset

Temuan selanjutnya adalah distribusi dari Response Code berhasil dengan kode 00 berjumlah 197.108 transaksi (98,30%), lalu Response Code transaksi dengan saldo tidak cukup dengan kode 51 berjumlah 3.413 transaksi (1,70%), pada dataset juga ditemukan flag transaksi normal dengan status 0 pada dataset berjumlah 199.793 transaksi (99,64%) , transaksi dengan status reversal atau dibatalkan dengan alasan timeout pada database berjumlah 728 transaksi (0,36%). Dari presentase data diatas dapat disimpilkan tingkat keberhasilan transaksi yang sangat tinggi menunjukkan sistem ATM yang reliable, reversal rate yang rendah mengindikasikan sistem yang stabil dengan sedikit masalah teknis. Hal ini juga menjadi informasi penting untuk *feature engineering* dimana kombinasi response code dan flag transaksi menjadi indikator fraud yang kuat. Selanjutnya pada **Gambar 4.3** berikut menunjukkan hasil yang merupakan pengujian training dan testing dataset yang digunakan dalam penelitian ini.



Gambar 4.3. Hasil pengujian training dan testing dataset

Berdasarkan gambar diatas, dataset dibagi dengan baik (80:20) dan stratified sehingga distribusi fraud tetap konsisten. Dengan feature engineering menambah informasi penting (temporal & perilaku), lalu diseleksi menjadi 46 fitur yang relevan. Analisis temporal menunjukkan pola fraud yang signifikan: lebih

tinggi pada weekend dan malam hari, sehingga fitur waktu sangat krusial dalam model deteksi fraud. Dengan struktur ini, dataset siap digunakan untuk melatih model machine learning yang lebih akurat dan robust.

4.2.1 Feature Engineering dan Pemilihan Fitur

Sebelum melakukan feature engineering peneliti terlebih dahulu melakukan analisis temporal pada distribusi transaksi per hari dengan distribusi transaksi yang terjadi pada hari jumat sebanyak 36.128 transaksi (18,02%), pada hari kamis transaksi yang terdistribusi sebanyak 35.610 transaksi (17,76%), hari senin sampai rabu 34.500 transaksi dan pada hari minggu 27.341 transaksi (13,63%). Peneliti juga mengamati distribusi transaksi per waktu transaksi diketahui transaksi yang terjadi pada pagi hari pukul 06.00 – 11.59 sebanyak 75.756 transaksi (37,78%), transaksi yang terjadi sore hari pukul 15:00-17.59 sebanyak 44.056 transaksi (21.97%), lalu transaksi yang terjadi pada malam hari pukul 18.00-20.59 sebanyak 34.288 transaksi (17,10%) dan transaksi yang terjadi pada dini hari yaitu pukul 00.00 – 05.59 sebanyak 5.886 transaksi (2,94%). Berdasarkan pola temporal yang diamati menunjukkan aktivitas normal pada jam kerja dan hari kerja. Transaksi yang terjadi pada dini hari bisa menjadi indicator potensial fraud karena transaksi terjadi pada jam tidak umum. Pola temporal ini juga menjadi basis untuk membuat fitur is_weekend, is_bussiness_hours,is_night_time yang dapat membantu model mengidentifikasi transaksi mencurigakan berdasarkan waktu terjadinya transaksi.

Feature engineering adalah tahap paling krusial dan kompleks dalam pengembangan system fraud detection. Tahap ini mengubah 24 fitur asli menjadi 70 fitur yang lebih informatif melalui ekstraksi pola, transformasi dan agregasi.

Fitur yang dibuat peneliti karena hasil EDA yang sebelumnya dilakukan adalah fitur transaksi dibuat dengan melakukan mapping dari kode transaksi kode_tx, fitur yang terbuat adalah tx_name memuat nama transaksi seperti penarikan tunai, transfer, dan cek saldo. Fitur kategori yaitu kategori transaksi seperti withdrawal, transfer, cek saldo, dan payment. Peneliti juga membuat fitur account_type yang merupakan jenis rekening pada dataset ini terdapat tabungan dan giro. Hal ini akan memudahkan model mengenali pola fraud berdasarkan kategori transaksi dibandingkan kode numerik yang ada pada database sebelumnya. Peneliti juga memasukkan pengetahuan domain perbankan ke dalam fitur sehingga memungkinkan model untuk belajar bahawa jenis transaksi tertentu misalnya penarikan tunai pada malam hari dengan nilai besar memiliki resiko fraud yang lebih tinggi.

Fitur kedua yang dibuat adalah fitur response code dan flag transaksi dimana fitur yang dibuat adalah rcode_desc yaitu deskripsi response code seperti transaksi sukses, saldo tidak cukup, System_error. Fitur selanjutnya adalah is_success yaitu binary flag 1 jika transaksi berhasil dilakukan, fitur is_failed yaitu binary flag 1 jika transaksi gagal, fitur flag_desc yaitu deskripsi flag transaksi yaitu normal atau reversal. Kombinasi fitur ini dilakukan karena kombinasi failure dan reversal merupakan indikator percobaan fraud lalu mengubah kategorikal menjadi angka berfungsi untuk memudahkam model tree based membuat keputusan.

Fitur ketiga adalah fitur temporal yang diekstraksi dari kolom tgl_tx dan jam_tx pada dataset untuk menangkap pola waktu transaksi. Fitur yang terbuat dari pola temporal terbagi menjadi beberapa bagian yaitu fitur tanggal yang didalamnya

ada year,month,day sebagai komponen tanggal, day_of_week hari dalam minggu, fitur day_name fitur nama hari seperti senin, selasa, rabu, kamis, dan jumat. Is_weekend yaitu bernilai 1 jika sabtu atau hari minggu. Is_Monday adalah binary flag bernilai 1 jika hari senin. Is_Friday binary flag bernilai 1 jika hari jumat. Selanjutnya peneliti membentuk fitur waktu dimana ada hour,minute,second komponen waktu yang diekstraksi dari jam_tx, lalu dibuat juga fitur time_category seperti dini hari (00.00-05.59), pagi (06.00-11.59), siang (12.00-14.59), sore (15:00-17:59), malam (18:00-20:59) dan malam_hari (21:00-23:59). Fitur selanjutnya yang ditemukan peneliti adalah fitur jam operasional yang dibagi menjadi tiga yaitu is_business_hours bernilai 1 jika transaksi dilakukan pada pukul 08.00-16:59 pada weekday, is_night_time bernilai 1 jika transaksi dilakukan pada pukul 22.00-05.59, lalu ada fitur is_early_morning bernilai 1 jika transaksi dilakukan 00.00-05.59. mengapa fitur temporal ini sangat penting karena pelaku fraud cenderung beroperasi di luar jam operasional atau pada *night time* untuk menghindari deteksi pada transaksi fraud.

Fitur yang keempat adalah fitur jumlah transaksi dimana fitur yang dibentuk adalah jumlah_tx_log adalah log transformasi dari jumlah transaksi. Fitur amount category yaitu fitur kategorisasi jumlah transaksi dikelompokkan sebagai berikut very_small jumlah nominal transaksi < Rp 100.000, small nominal transaksi dengan jumlah antara Rp 100.000 – Rp 500.000, medium transaksi jika jumlah nominal transaksi antara Rp 500.000 – Rp 1.000.000, large transaksi jika jumlah nominal transaksi Rp 1.000.000 – Rp 5.000.000 dan very_large jika nominal transaksi > Rp 5.000.000. fitur is_round_amount yaitu binary flag untuk transaksi dengan nilai

bulat. Peneliti juga membuat balance fitur yang di dalamnya terdapat saldo_akhir_log sebagai log transformasi dari saldo akhir, fitur has_negative_balance untuk flag saldo negative jika ada tetapi dalam dataset 0 kasus, low_balance yaitu flag untuk saldo < Rp 100.000. selanjutnya ditemukan juga fitur ratio yang berisi informasi rasio jumlah transaksi terhadap saldo dengan formula jumlah_tx / saldo_akhir sehingga menemukan apabila ratio tinggi berarti potensi resiko fraud juga tinggi.

Fitur yang kelima adalah fitur bank dan lokasi transaksi fitur yang dibuat adalah is_same_bank yang bernilai 1 jika transaksi terjadi pada kode bank yang sama, fitur is_cross_bank yang bernilai 1 jika transaksi antar bank, fitur is_home_branch yang bernilai 1 jika transaksi dilakukan pada cabang asal rekening. Fitur has_destination yang bernilai 1 jika transaksi memiliki rekening tujuan. Fitur has_kd_bank_tujuan yang bernilai 1 jika ada kode bank tujuan. Fitur ini dibentuk dengan tujuan fraud terjadi pada transfer antar bank, maka kombinasi transfer antar bank lalu transaksi dilakukan pada malam hari dengan jumlah transaksi yang sangat besar adalah potensi fraud yang sangat besar.

Fitur keenam adalah fitur customer behavior yang dibuat peneliti seperti card_tx_count dimana fitur ini berisi informasi pengunaan kartu untuk menunjukkan seberapa aktif kartu digunakan oleh nasabah. Fitur is_frequent_card merupakan fitur yang berfungsi untuk mengetahui kartu yang sangat jarang digunakan. Fitur selanjutnya adalah fitur account_tx_count yaitu fitur yang berisi informasi frekuensi transaksi per rekening. Fitur ini dapat membantu model membedakan transaksi dengan perilaku normal seperti kartu atm regular

bertransaksi pada jam operasional dengan jumlah transaksi kecil dan untuk transaksi mencurigakan fraud pada kondisi transaksi kartu lama yang jarang digunakan mulai bertransaksi pada malam hari dengan jumlah transaksi yang sangat besar.

Fitur ketujuh yang dibuat peneliti adalah fitur fraud indicator antara lain fitur failed_and_reversal, fitur ini digunakan untuk transaksi yang gagal dan reversal. Fitur large_weekend_withdrawal sebagai fitur untuk mengenal penarikan besar di weekend. Fitur night_hight_value yaitu fitur yang digunakan untuk mendeteksi transaksi bernilai tinggi di malam hari. Selanjutnya ada fitur is_sequntial yang merupakan fitur yang dapat mendeteksi transaksi pengunaan kartu berturut turut. Selanjutnya fitur large_weekend_withdrawal adalah fitur yang diperuntukkan penarikan besar di weekend. Lalu, ada fitur night_high_value yang menyimpan karakteristik nasabah bertransaksi bernilai tinggi pada malam hari. berdasarkan pola fraud yang nyata terjadi di perbankan fraud terjadi penarikan besar di akhir pekan dikarenakan keamanan yang lebih rendah di akhir pekan.

Setelah melakukan *feature engineering* menghasilkan 70 fitur, tahap selanjutnya adalah memilih fitur yang relevan untuk pemodelan. Pada penelitian ini mengunakkan 46 fitur.Tahap ini peneliti mengunakkan original fitur seperti: jumlah_tx, saldo_akhir, kd_bank_loktx, kd_bank_lokrek, kd_cab_rek, opendate, jenistx alasan peneliti mengunakkan fitur ini karena fitur ini merupakan atribut dasar transaksi yang mengandung informasi penting tentang karakteristik transaksi, kemudian kode cabang dan jenis transaksi memberikan konteks bisnis yang dapat mengidentifikasi pola lokasi atau jenis transaksi yang rentan fraud. Selanjutnya

peneliti mengunakkan fitur temporal seperti: month, day, day_of_week, hour, minute, is_weekend, is_Monday, is_Friday,is_bussiness_hours, is_night_time, is_early_morning alasan peneliti mengambil fitur ini karena fraud memiliki pola waktu tertentu contoh malam hari, weekend, diluar jam kerja berbeda dengan transaksi normal cenderung terjadi pada jam kerja. Fitur transaksi menjadi pilihan peneliti dengan fitur jumlah_tx_log, is_high_value, is_round_amount dengan alasan memberi tanda transaksi di atas ambang batas dan mengambil nilai pecahan bulat saat transaksi. Selanjutnya peneliti mengambil fitur saldo antara lain: saldo_akhir_log, has_negative_balance, low_balance, dan tx_to_balance_ratio karena saldo mencerminkan kondisi rekening, selain itu ratio transaksi terhadap saldo sangat penting yang memahami pola fraud yang cenderung menguras saldo.

Fitur selanjutnya yang diambil oleh peneliti adalah fitur kode respon seperti rcode,is_success,is_failed karena response code menunjukkan hasil transaksi, kombinasi transaksi sukses dan transaksi gagal juga dapat mengidentifikasi transaksi anomaly. Selanjutnya peneliti mengunakkan fitur flag seperti: flag_tx, is_reversal alasan mengambil fitur ini transaksi dengan reversal berlebihan atau pada waktu mencurigakan merupakan potensial fraud. Selanjutnya peneliti memilih fitur bank seperti: is_same_bank, is_cross_bank, has_destination, has_kd_bank_tujuan dengan alasan pelaku fraud biasanya mengunakkan akun bank lain untuk memindahkan dananya sehingga transaksi antar bank dengan jumlah besar merupakan resiko terjadinya fraud. Selanjutnya peneliti mengunakkan fitur perilaku nasabah seperti: card_tx_count, is_frequent_card, account_tx_count dengan alasan frekuensi pengunaan kartu atm dapat mengetahui pola transaksi

nasabah, selain itu fitur ini dapat membedakan nasabah yang aktif dan nasabah yang dormant.

Fitur yang selanjutnya adalah fitur indikator fraud seperti: failed_and_reversal, large_weekend_withdrawal, night_high_value, is_sequential, risk_score. Pemilihan fitur indikator fraud berdasarkan pengetahuan pada pola yang fraud yang pernah terjadi pada Bank Sultra yaitu pelaku fraud skimming melakukan aksinya pada tengah malam sekitar pukul 00.00 – 05.59 pada beberapa titik atm secara berkelompok lalu melakukan transaksi dengan jumlah maksimal transfer lalu ditransfer ke aku bank lain. Fitur akhir yang digunakan peneliti adalah fitur kategorial seperti tx_category, account_type, time_category, amount_category dengan alasan fitur ini mengelompokkan nilai secara berkelanjutan sehingga semua transaksi yang dilakukan dapat dikategorikan untuk menjadi dasar penilaiaan risiko fraud.

4.2.2 Penanganan Imbalanced Data dengan SMOTE

Pada tahap ini peneliti mengatasi ketidakseimbangan kelas yang ekstrim pada dataset transaksi ATM Bank Sultra dengan mengunakkan SMOTE (Synthetic Minority Over-sampling Technique) sebagai teknik resampling. SMOTE dipilih karena kemampuannya menghasilkan synthetic sample melalui interpolasi k-nearest neighbors, sehingga tidak sekedar menduplikasi data fraud yang sudah ada, melainkan menciptakan variasi baru yang memperkaya representasi kelas minoritas. Pendekatan ini lebih efektif dibandingkan random oversampling konvensional karena mengurangi risiko overfitting dan meningkatkan kemampuan dalam mengeneralisasi model dalam mendeteksi pola fraud yang beragam.

Implementasi SMOTE pada penelitian ini mengunakkan parameter k_neighbors=5 dan sampling_strategy='auto' yang secara otomatis menyeimbangkan kelas minoritas (fraud) dengan kelas mayoritas (non-fraud) pada rasio 1:1. Dari 9.433 sampel fraud asli dalam training set, SMOTE berhasil menghasilkan 141.551 synthetic sampel melalui interpolasi linear antara fraud sampel dengan 5 tetangga terdekatnya, sehingga total fraud sample menjadi 150.983 yang seimbang dengan jumlah non fraud. Sangat penting pada proses ini peneliti hanya menerapkan pada training set setelah proses train split, sementara test set yang bernilai 20% tetap mempertahankan distribusi kelas asli dengan imbalance rasio 1:16. Strategi ini digunakan untuk menghindari data leakage dan memastikan evaluasi model dilakukan pada kondisi yang realistis sesuai dengan karakteristik data real production.

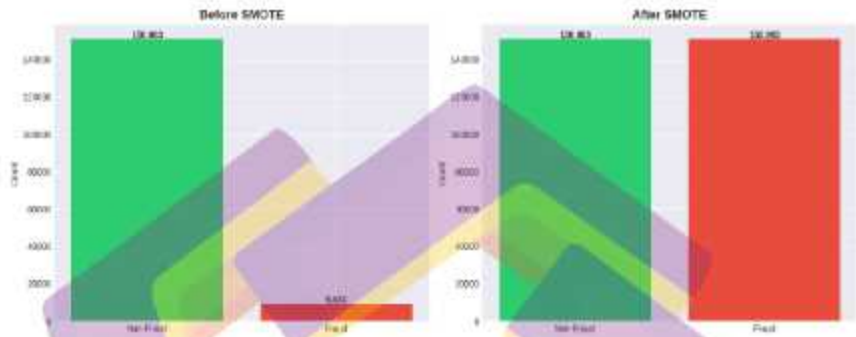
Hasil penerapan SMOTE menjukkan keberhasilan menciptkan training set yang balanced dengan total record 301.786 record dengan komposisi 150.983 data fraud dan 150.983 data non fraud. Memberikan model kesempatan yang setara untuk mempelajari karakteristik kedua kelas. Validasi teknis menjukkan bahawa parameter k_neighbors=5 memenuhi syarat minimal yaitu k < jumlah fraud sample dan synthetic sampel yang dihasilkan memiliki distribusi fitur yang konsisten dengan fraud sampel asli. Pendekatan ini memungkinkan algoritma machine learning untuk mengidentifikasi pola fraud dengan lebih baik tanpa bias terhadap kelas mayoritas sekaigus mempertahankan integritas evaluasi model melalui test set yang tidak dimodifikasi.

Proses untuk mengatasi ketidakseimbangan kelas pada dataset dengan membuat sampel sintetis untuk kelas minoritas (Astuti & Lenti, 2021). Keunggulan dari menggunakan SMOTE pada dataset yang tidak seimbang ini adalah, akan meningkatkan jumlah sampel di kelas minoritas (*anomaly*) sehingga model tidak hanya berfokus pada kelas mayoritas (normal), mengurangi false negative, sehingga lebih banyak anomaly yang terdeteksi, meningkatkan AUC (*Area Under Curve*) dalam ROC Curve yang menunjukkan model lebih baik dalam membedakan kelas, nilai dari precision, recall, dan f1-score lebih seimbang antara kelas mayoritas dan minoritas sehingga akan mempengaruhi hasil dari akurasi.

SMOTE membantu model ML agar tidak hanya "belajar" dari kelas mayoritas, sehingga meningkatkan kemampuan model dalam mengenali dan memprediksi data dari kelas minoritas. Perlu dicatat bahwa SMOTE hanya diterapkan pada training set untuk menghindari data leakage, sedangkan test set tetap mempertahankan distribusi original untuk evaluasi yang realistis terhadap kondisi nyata. Setelah pembagian data selesai, pemodelan akan dilakukan menggunakan tiga algoritma ML, yaitu SVM, RF, K-NN dengan *ensemble Hard Voting* (HV) dan *Soft Voting* (SV).

Penerapan SMOTE hanya pada data training bertujuan untuk meningkatkan kinerja model saat pelatihan, bukan untuk memanipulasi data pengujian (test data). Jika SMOTE diterapkan pada seluruh dataset sebelum pembagian, maka data sintetis akan bocor ke data test, menyebabkan evaluasi model menjadi tidak valid karena data test tidak lagi mewakili kondisi dunia nyata. Oleh karena itu, SMOTE harus dilakukan setelah data dibagi, hanya pada data training agar hasil evaluasi

tetap objektif dan tidak terjadi data leakage. Pemodelan ini akan dilakukan tanpa *Hyperparameter Tuning* dengan hasil SMOTE ditunjukkan pada **Gambar 4.4.** berikut.



Gambar 4.4. Hasil Pengujian SMOTE

Keadaan sebelum SMOTE sejalan dengan banyak penelitian fraud detection yang menegaskan bahwa ketidakseimbangan kelas dapat menyebabkan nilai akurasi tampak tinggi tetapi recall atau sensitivity untuk kelas fraud sangat rendah, karena model lebih sering "benar" hanya dengan memprediksi non-fraud. Studi-studi terkini mengenai deteksi fraud keuangan menunjukkan bahwa teknik oversampling berbasis SMOTE mampu meningkatkan kemampuan model dalam mengenali kelas minoritas dengan cara menghasilkan sampel sintetis di sekitar tetangga terdekat kelas fraud, bukan sekadar menduplikasi data yang sudah ada, sehingga distribusi fitur menjadi lebih representatif untuk proses pelatihan.

Berdasarkan **Gambar 4.4.** diatas, menunjukkan perubahan distribusi kelas *non-fraud* dan *Fraud* sebelum dan sesudah penerapan SMOTE pada data transaksi ATM. Sebelum SMOTE, jumlah transaksi *non-fraud* jauh lebih besar (150.983) dibanding *Fraud* (9.433), sehingga dataset sangat imbalanced dan

cenderung membuat model belajar "bermain aman" dengan lebih sering memprediksi kelas mayoritas. Setelah SMOTE, kelas *Fraud* dibuat seimbang dengan *non-fraud* (keduanya 150.883), sehingga algoritma machine learning akan mendapat sinyal yang lebih kuat tentang karakteristik transaksi fraud.

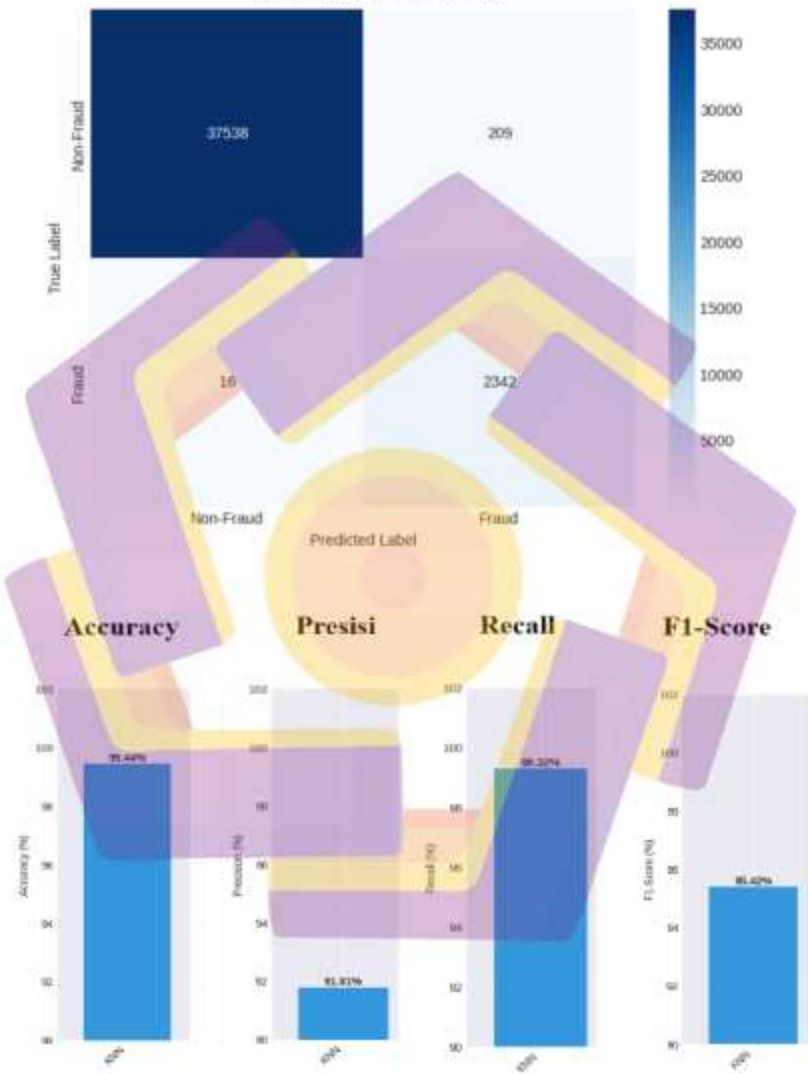
Penelitian (Pratama et al., 2023) sebelumnya pada domain fraud perbankan dan kartu kredit melaporkan bahwa penggunaan SMOTE atau varian ensemble-oversampling mampu meningkatkan metrik seperti recall, F1-score, dan AUC untuk kelas fraud dibandingkan pelatihan pada data asli yang imbalanced. Beberapa studi juga menekankan bahwa ketika data sudah diseimbangkan, model seperti Random Forest, SVM, dan KNN atau ensemble voting (hard/soft) dapat memanfaatkan pola pada kelas fraud dengan lebih baik, sehingga trade-off antara *false negative* (fraud lolos) dan *false positive* (transaksi normal salah deteksi) menjadi lebih terkendali.

4.3 Pemodelan Data

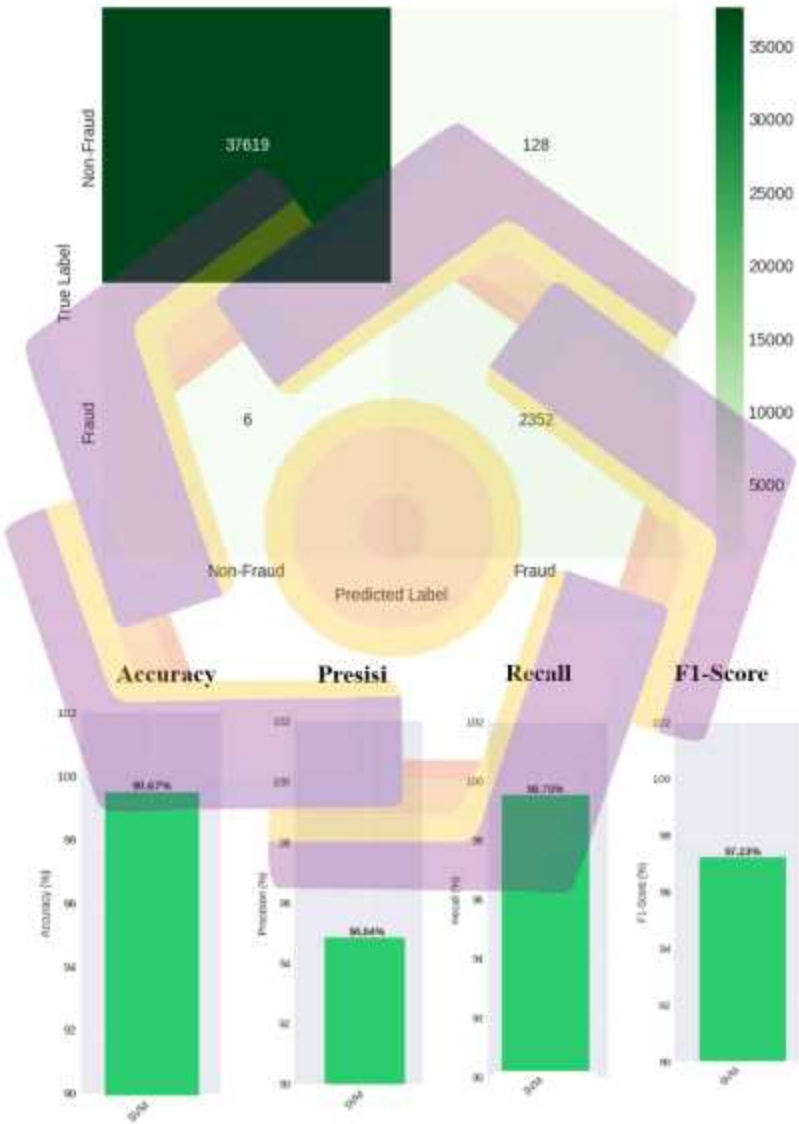
Pemodelan dalam penelitian ini menggunakan 3 jenis model algoritmik ML, yaitu; SVM, RF, K-NN dengan ensemble menggunakan Hard Voting dan Soft Voting. Pemodelan ini merujuk pada konseptual, logis dan fisik. Tujuan utama dari pemodelan ini adalah untuk mengorganisasi dan menstrukturkan data mentah ke dalam format yang sesuai agar model machine learning dapat belajar, mengidentifikasi pola, dan menghasilkan prediksi yang akurat (Ramadhani et al., 2025). Pada **Gambar 4.5** berikut disajikan hasil pengujian dari masing-masing model algoritmik ML yang digunakan dalam pemodelan data penelitian ini.

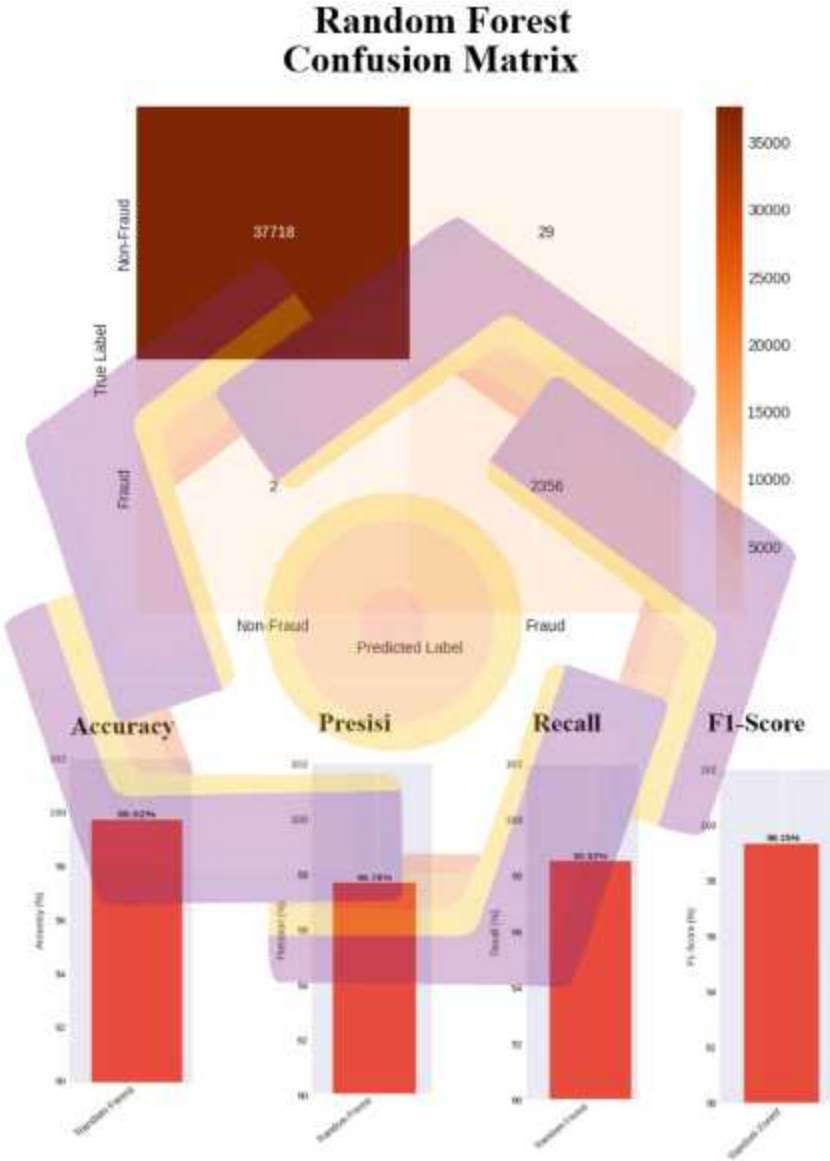
K-Nearst Neighbors

Confusion Matrix

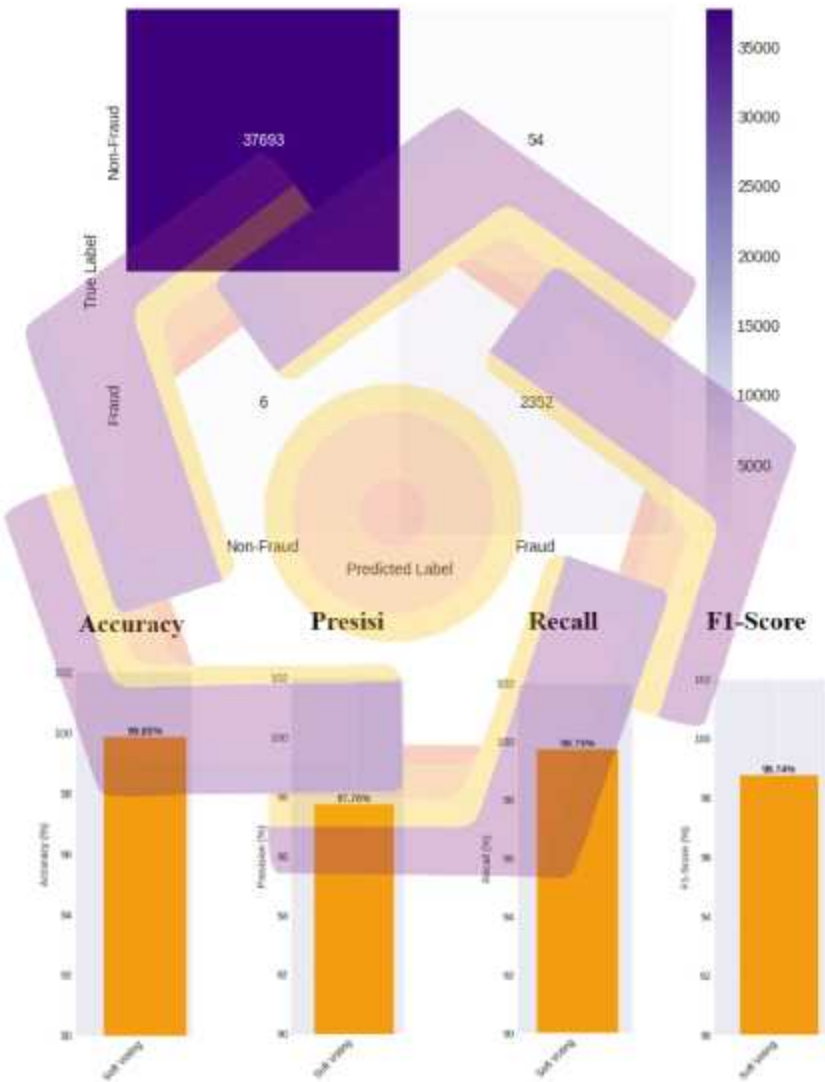


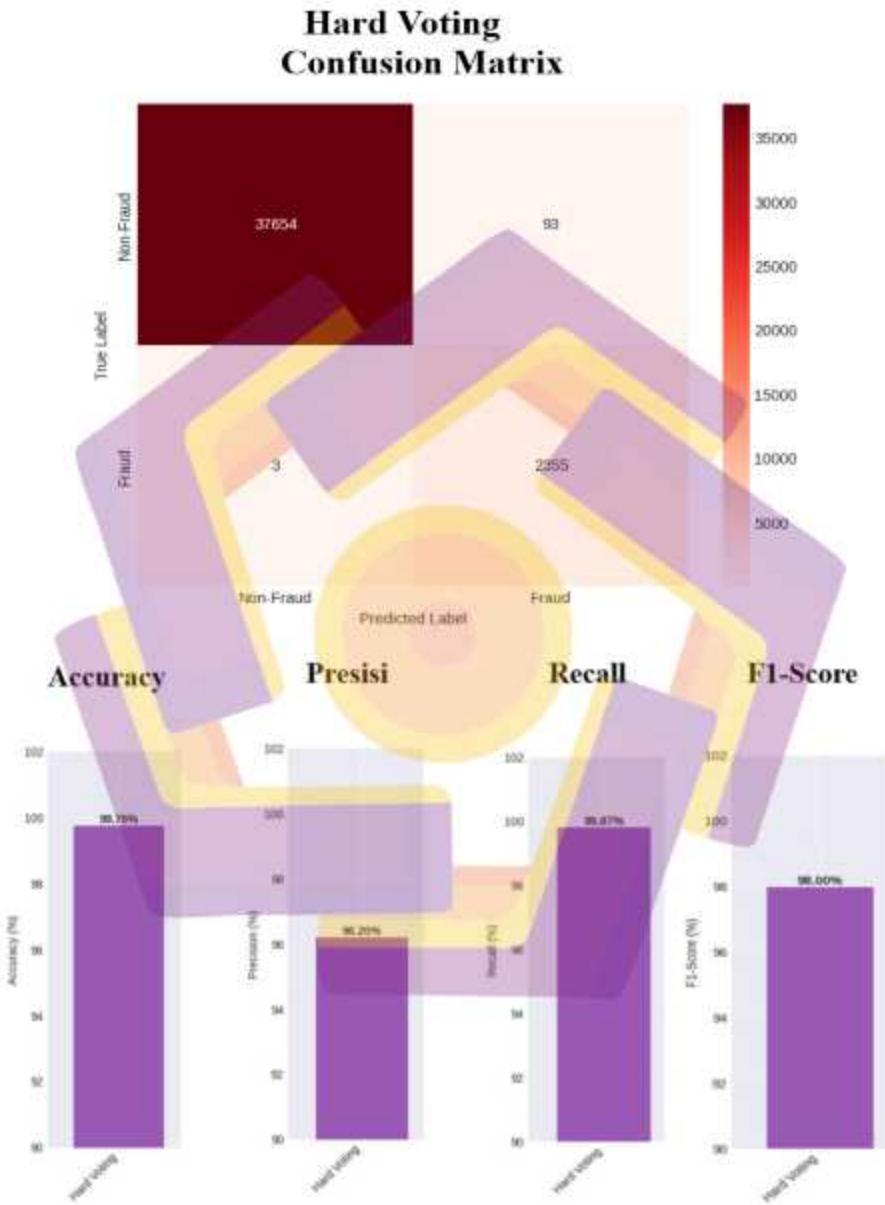
Support Vector Machine
Confusion Matrix




Random Forest
Confusion Matrix
37718
29
2
2356
Non-Fraud
Fraud
True Label
Non-Fraud
Fraud
Predicted Label
35000
30000
25000
20000
15000
10000
5000
Accuracy
Presisi
Recall
F1-Score

Soft Voting
Confusion Matrix





Gambar 4.5. Nilai Confusion Matrix Hasil Penelitian

Berdasarkan hasil pengujian seperti yang ditunjukkan pada **Gambar 4.5** diatas, kelima algoritma ML menunjukkan bahwa nilai f1-score yang rata-rata mendekati = 1 yang berarti bahwa model klasifikasi ini memiliki kinerja yang sangat baik untuk data fraud yang digunakan dalam penelitian ini. Hal ini juga menunjukkan bahwa model tersebut memiliki presisi yang akurat. Namun demikian dari kelima model ML ini nilai f1-score yang terbaik ditunjukkan oleh RF dengan nilai sebesar 0,9935, ini menunjukkan bahwa algoritma dengan kinerja paling baik memiliki keseimbang antara presisi dan recall yang baik pula. Nilai 0,99 ini berarti model RF mampu mengidentifikasi sebagian besar kasus positif dengan benar (recall yang baik) pada saat yang sama, tidak sering salah mengklasifikasikan kasus negatif sebagai positif (presisi yang baik).

Berdasarkan pada **Gambar 4.5** diatas menunjukkan bahwa keseluruhan nilai pengujian dengan confusion matrix dari masing-masing model ML memiliki nilai metrik yang menunjukkan bahwa masing-masing model sudah bekerja sangat baik untuk deteksi fraud. Angka F1-Score, akurasi, presisi, recall, dan ROC-AUC pada **Gambar 4.6** menunjukkan semuanya sangat tinggi (di atas 0,95), sehingga jumlah salah klasifikasi (FP dan FN) pada confusion matrix relatif sangat kecil untuk semua algoritma. Dengan akurasi mendekati 1 artinya hampir semua transaksi (fraud dan non-fraud) diklasifikasikan dengan benar, presisi tinggi (≈0,92–0,99) artinya dari semua transaksi yang diprediksi sebagai fraud, sebagian besar memang benar-benar fraud (FP sedikit), recall sangat tinggi (≈0,99) artinya hampir semua transaksi fraud berhasil terdeteksi (FN sangat sedikit), F1-Score tinggi menunjukkan keseimbangan yang baik antara presisi dan recall, ROC-AUC

mendekati 1 menandakan pemisahan yang sangat baik antara kelas fraud dan non-fraud.

Hasil penelitian dari **Gambar 4.5** menunjukkan bahwa Model ini hampir selalu berhasil mendeteksi transaksi fraud (recall sangat tinggi), dengan presisi juga sangat baik sehingga *false positive* rendah. Kombinasi tersebut membuat F1 dan ROC-AUC pada **Gambar 4.6** menunjukkan nilai yang mendekati 1, menandakan SVM sangat efektif sebagai pendeteksi fraud. Sedangkan RF adalah model terbaik: akurasi hampir 100%, recall nyaris sempurna, dan presisi lebih tinggi dari SVM. Artinya, RF bukan hanya mampu menangkap hampir semua fraud, tetapi juga sangat jarang salah menandai transaksi normal sebagai fraud.

KNN memiliki recall yang tetap sangat tinggi (banyak fraud terdeteksi), tetapi presisi lebih rendah dibanding SVM dan RF, menunjukkan jumlah *false positive* lebih besar. F1 masih tinggi, namun agak di bawah dua model sebelumnya. Hard voting yang menggabungkan label mayoritas SVM, RF, dan KNN menghasilkan recall yang tetap sangat tinggi dengan presisi yang sedikit lebih baik daripada SVM. Ini menunjukkan ensemble mampu menstabilkan prediksi antar model, mengurangi kesalahan satu model dengan "suara" model lain. Hard voting yang menggabungkan label mayoritas SVM, RF, dan KNN menghasilkan recall yang tetap sangat tinggi dengan presisi yang sedikit lebih baik daripada SVM. Ini menunjukkan ensemble mampu menstabilkan prediksi antar model, mengurangi kesalahan satu model dengan "suara" model lain.

Soft voting mengambil rata-rata probabilitas dari semua model, sehingga dapat memanfaatkan "tingkat keyakinan" masing-masing model. Hasilnya, presisi

dan recall sama-sama sangat tinggi dan seimbang, sedikit di bawah RF tunggal tetapi di atas SVM, KNN, dan hard voting dalam hal F1. Ini menunjukkan ensemble probabilistik memberikan kompromi yang sangat baik antara deteksi fraud maksimal dan minimnya alarm palsu. Secara praktis, semua model berada pada zona "sangat baik", tetapi RF dan Soft Voting dapat ditonjolkan sebagai model dengan kinerja paling seimbang dan stabil untuk sistem deteksi fraud ATM.

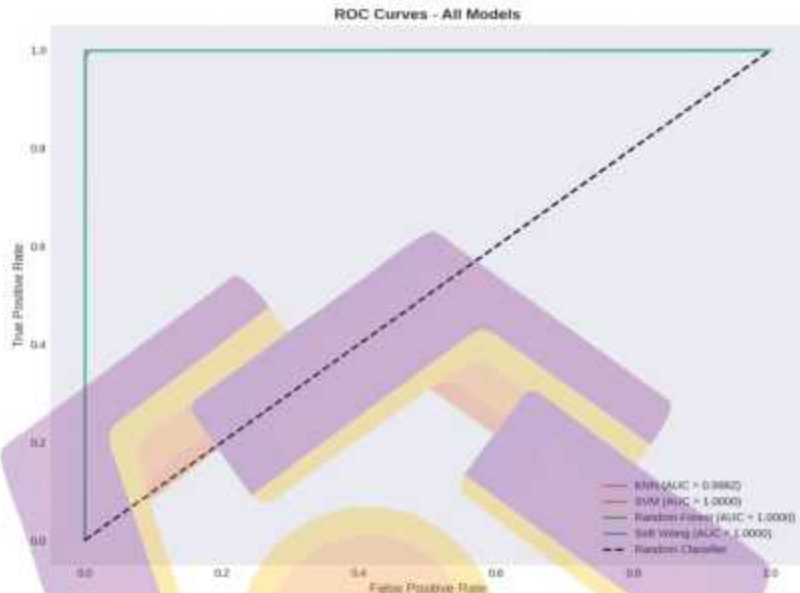
Studi (Andrade-Arenas & Yactayo-Arias, 2025) mengenai fraud kartu kredit dan transaksi perbankan melaporkan bahwa Random Forest dan SVM biasanya termasuk model terbaik, dengan akurasi sekitar 0,96–0,99 dan ROC-AUC sekitar 0,95–0,99 pada data imbalanced yang sudah diatasi dengan SMOTE atau teknik serupa. Penelitian lain oleh (Osmond, 2025) yang mengevaluasi berbagai model (Random Forest, XGBoost, Logistic Regression dan KNN) menunjukkan bahwa Random Forest sering mencapai akurasi 0,999, F1 sekitar 0,87, dan ROC-AUC sekitar 0,98 pada tugas deteksi fraud keuangan, mengonfirmasi bahwa model berbasis ensemble cenderung unggul.

Studi terbaru oleh (Ahmed et al., 2025) mengenai ensemble soft voting dan model voting lainnya pada deteksi fraud menunjukkan bahwa menggabungkan beberapa algoritma (misalnya RF, SVM, KNN) dengan skema soft voting mampu meningkatkan F1 dan AUC dibanding model tunggal, terutama setelah penyeimbangan kelas seperti SMOTE/SMOTE-ENN. Dibandingkan angka tersebut, hasil penelitian Anda (F1 $\geq$ 0,95 dan ROC-AUC $\approx$ 0,999 untuk hampir semua model) berada di atas atau setidaknya setara dengan performa terbaik di

literatur, yang dapat dijelaskan oleh penggunaan teknik penyeimbangan data, pemilihan fitur yang baik, dan pengaturan hiperparameter yang optimal.

Secara metrik, model ini tidak hanya konsisten dengan tren literatur yang menempatkan Random Forest dan ensemble voting sebagai pendekatan unggul, tetapi bahkan menunjukkan peningkatan nilai F1 dan ROC-AUC. Hal ini mengindikasikan bahwa kombinasi penanganan class imbalance (misalnya SMOTE) dan ensemble (khususnya Random Forest dan Soft Voting) sangat efektif untuk konteks deteksi fraud ATM.

Selanjutnya untuk kurva ROC-AUC seperti yang ditunjukkan pada **Gambar 4.6** berikut yang dihasilkan dalam penelitian ini menunjukkan bahwa performa pemisahan kelas fraud dan non-fraud untuk KNN, SVM, RF dengan Soft Voting yang semuanya berada sangat dekat dengan sudut kiri atas sehingga garisnya hampir vertikal di FPR ≈ 0 lalu horizontal di TPR ≈ 1. Hal ini berarti untuk hampir semua nilai threshold, model mampu mempertahankan *true positive rate* (recall) yang sangat tinggi sekaligus *false positive rate* yang sangat rendah, yang tercermin dari nilai AUC ≈ 0,9982 untuk KNN dan 1,0000 untuk SVM, Random Forest, dan Soft Voting.



Gambar 4.6. Kurva ROC-AUC

Penelitian sebelumnya oleh (Aghware et al., 2024) menyatakan bahwa AUC yang mendekati 1 diartikan sebagai kemampuan diskriminasi yang hampir sempurna antara kelas positif (fraud) dan negatif (non-fraud), jauh di atas garis putus-putus diagonal yang menggambarkan *random classifier* dengan AUC = 0,5. Studi-studi deteksi fraud kartu kredit dan transaksi finansial melaporkan bahwa penggunaan model kuat seperti Random Forest, SVM, dan ensemble voting pada data yang sudah ditangani ketidakseimbangannya (misalnya dengan SMOTE/varian) dapat menghasilkan ROC-AUC sangat tinggi (sekitar 0,97–0,99), yang sejalan namun sedikit di bawah kinerja yang Anda peroleh. Dengan demikian, kurva ROC ini dapat dijadikan argumen kuat bahwa kombinasi algoritma dan strategi prapemrosesan yang digunakan dalam penelitian ini menghasilkan sistem

deteksi fraud ATM yang hampir optimal dalam memisahkan transaksi fraud dan non-fraud.

4.3.1 Evaluasi, Verifikasi, Validasi Sistem dan Model

Selanjutnya dilakukan evaluasi, verifikasi, dan validasi terhadap pengujian yang telah dilakukan sehingga didapatkan hasil penelitian yang menunjukkan bahwa semua algoritma yang digunakan mampu mendeteksi transaksi fraud dengan sangat baik, dengan model terbaik adalah RF dan peningkatan kinerja melalui Voting Classifier, terutama soft voting. Hal ini sejalan dengan hasil penelitian yang dilakukan oleh (Syahbani et al., 2025) hasilnya menunjukkan bahwa algoritma ensemble, khususnya Random Forest dan XG-Boost, memberikan performa terbaik untuk deteksi fraud transaksi keuangan dibanding algoritma klasik lainnya, dengan catatan bahwa kualitas praproses data sangat menentukan hasil akhir. Dengan teknik praproses data seperti SMOTE terbukti sangat berpengaruh terhadap kemampuan model dalam mengenali fraud dan menekan false positive.

Random Forest memperoleh F1-score sekitar 0,9935 dan akurasi 0,9992, dengan confusion matrix menunjukkan 37.718 transaksi non-fraud dan 2.356 transaksi fraud diklasifikasikan benar, serta hanya 29 false positive dan 2 false negative. Nilai presisi dan recall keduanya mendekati 1 menandakan RF hampir tidak salah memberi label fraud maupun meloloskan fraud, sejalan dengan literatur yang menyatakan RF sangat efektif untuk deteksi fraud karena sifat ensemble dan kemampuannya menangani data tidak seimbang.

SVM menunjukkan F1-score sekitar 0,9723 dengan akurasi 0,9967, sedangkan KNN memiliki F1-score sekitar 0,9542 dan akurasi 0,9944; keduanya

masih sangat baik tetapi sedikit di bawah RF. Temuan ini konsisten dengan penelitian yang melaporkan bahwa pada data transaksi yang kompleks dan cenderung imbalanced, algoritma tree-based ensemble seperti Random Forest umumnya mengungguli model margin-based (SVM) dan distance-based (KNN) dalam hal stabilitas dan kemampuan generalisasi. Hard voting menghasilkan F1-score sekitar 0,9800 dan akurasi 0,9976, menunjukkan bahwa penggabungan suara ketiga model sudah mampu mengurangi sebagian kesalahan masing-masing model tunggal. Soft voting memberikan F1-score sekitar 0,9874 dan akurasi 0,9985 dengan ROC-AUC mendekati 1, yang berarti kombinasi probabilitas prediksi SVM, Random Forest, dan KNN menghasilkan pemisahan kelas fraud dan non-fraud yang hampir sempurna, sejalan dengan literatur bahwa soft voting cenderung lebih kuat karena memanfaatkan tingkat keyakinan masing-masing model.

Hasil di mana RF dan ensemble voting memberikan performa tertinggi selaras dengan berbagai studi fraud detection yang menunjukkan bahwa teknik ensemble, khususnya RF dan Voting Classifier, mampu meningkatkan F1-score dan ROC-AUC pada data transaksi finansial yang tidak seimbang. Dengan nilai F1-score dan ROC-AUC yang mendekati 1, penelitian ini memperkuat bukti bahwa kombinasi algoritma SVM, RF, KNN, dan Voting Classifier merupakan pendekatan yang sangat efektif untuk sistem deteksi fraud transaksi ATM, serta layak dipertimbangkan sebagai solusi praktis di lingkungan perbankan.

Kurva ROC untuk semua model yang digunakan dan menunjukkan bahwa kinerja deteksi fraud berada pada level sangat tinggi, bahkan mendekati sempurna. Kurva ROC untuk SVM, Random Forest, dan Soft Voting menempel di sisi kiri dan

atas grafik dengan nilai AUC = 1,0000, artinya pada berbagai threshold model mampu memaksimalkan true positive rate sambil meminimalkan false positive rate; secara praktis, model hampir tidak salah membedakan transaksi fraud dan non-fraud.

Kurva ROC KNN juga berada sangat dekat dengan tiga model lainnya dengan AUC = 0,9982, menunjukkan kemampuan klasifikasi yang nyaris sempurna meskipun sedikit di bawah tiga model utama. Garis putus-putus diagonal menunjukkan performa random classifier (AUC = 0,5); semua kurva model jauh di atas garis ini, menegaskan bahwa seluruh algoritma memberikan informasi klasifikasi yang sangat kuat dan layak digunakan untuk sistem deteksi fraud transaksi ATM.

Potensi penerapan model RF-SMOTE pada sistem real-time fraud monitoring dan integrasi ke sistem keuangan sangat menjanjikan untuk diintegrasikan pada sistem fraud detection real-time di dunia finansial. Dengan teknologi API, model bisa "menyaring" transaksi mencurigakan secara real-time dan scalable, memberikan proteksi proaktif pada transaksi konsumen dan lembaga keuangan. Hal ini karena kelebihan model RF-SMOTE memiliki deteksi kuat untuk Data Tidak Seimbang: Random Forest yang dilatih dengan data hasil balancing SMOTE mampu mendeteksi transaksi fraud walaupun proporsinya sangat kecil (misal <0,2%).

Studi empiris terbaru menunjukkan model ini memiliki akurasi 97–99,5% dan F1-score serta recall sangat tinggi, sehingga jarang melewatkan kasus fraud, ahan terhadap outlier, noise, dan tetap stabil saat memasukkan data baru, yang

sangat penting untuk transaksi keuangan real-time. Sehingga model dapat dimasukkan ke API scoring engine. Prosesnya: tiap transaksi masuk, fitur diekstrak dan distandarisasi, lalu model memprediksi skor fraud (atau langsung prediksi 0/1). Sehingga prediksi bisa dilakukan dalam hitungan milidetik—sesuai untuk sistem real-time (contohnya pada layanan transaksi online atau sistem alert bank).

4.3.2 Cross Validation

Untuk memvalidasi model ML yang telah dikembangkan, dalam penelitian ini digunakan 5-Fold Cross-Validation pada seluruh set pelatihan yang telah diimbangi dengan SMOTE. Validasi silang merupakan teknik validasi yang penting untuk menganalisa kinerja model secara lebih komprehensif dibandingkan single train-test split. Hal ini bertujuan untuk memastikan bahwa kinerja yang diobservasi tidak hanya hasil dari kebetulan nilai yang baik atau distribusi data spesifik dalam set pelatihan tertentu. Dalam 5-Fold Cross-Validation, training set dibagi menjadi 5 subset (folds) yang equal size, dimana model di-train pada 4 lipatan dan di-validasi pada sisa lipatan, dengan proses ini diulang 5 kali sehingga setiap pengujian memiliki nilai validation set yang sesuai. Metode ini menghasilkan 5 estimasi kinerja mandiri yang dapat digunakan untuk mendapatkan rata-rata kinerja model dan standar deviasi Hal ini memberikan wawasan tentang stabilitas dan konsistensi model di berbagai subset data.

Hasil validasi silang menunjukkan bahwa semua algoritma yang diuji mencapai kinerja yang sangat tinggi dan sangat stabil. Random Forest sebagai model terbaik menunjukkan CV mean F1-Score 99,93% dengan standar deviasi hanya 0,008%, ini menunjukkan konsistensi yang luar biasa tinggi dalam 5 kali

pengujian yang dilakukan. Stabilitas yang ditunjukkan melalui standar deviasi yang sangat rendah (<0.01%) menunjukkan bahwa kinerja model tidak sensitif terhadap komposisi spesifik dari data pelatihan di setiap pengujian, melainkan dapat digeneralisasikan. Support Vector Machine juga menunjukkan stabilitas yang sangat baik dengan CV mean F1-Score 99,78% (std: 0,022%), diikuti oleh Soft Voting dengan 99,91% (std: 0,010%), Hard Voting dengan 99,85% (std: 0,015%), dan K-Nearest Neighbours dengan 99,66% (std: 0,023%). Konsistensi kinerja tinggi di semua algoritma memvalidasi bahwa dataset seimbang dengan hasil SMOTE yang memberikan landasan sebagai pembelajaran ML, sehingga tidak menimbulkan data yang bias dan dapat mengganggu kestabilan kinerja model ML. Seperti yang ditunjukkan pada masing-masing **Tabel 4.2; Tabel 4.3; Tabel 4.4; Tabel 4.5;** dan **Tabel 4.6.** berikut sesuai dengan Algortima ML dan Pemodelan yang dihasilkan dari pengujian CV.

Tabel 4.2. Algoritma KNN

Parameter	Akurasi	Presisi	Recall	F1-Score
CV Mean	99,66 %	99,33%	100,00%	99,66%
CV Std Dev	0,024%	0,047%	0,003%	0,023%
Test Set	99,44%	91,81%	99,32%	95,42%
CV-Test Gap	0,22%	7,53%	0,68%	4,25%
Stability	Very Stable	Very Stable	Very Stable	Very Stable
Consistency	Consistent	Inconsistent	Consistent	Acceptable

Tabel 4.3. Algoritma SVM

Parameter	Akurasi	Presisi	Recall	F1-Score
CV Mean	99,78 %	99.58%	99,98%	99,78%
CV Std Dev	0,022%	0,038%	0,008%	0,022%
Test Set	99,67%	94,84%	99,75%	97,23%
CV-Test Gap	0,12%	4,74%	0,24%	2,55%
Stability	Very Stable	Very Stable	Very Stable	Very Stable
Consistency	Consistent	Acceptable	Consistent	Acceptable

Tabel 4.4. Algoritma Random Forest

Parameter	Akurasi	Presisi	Recall	F1-Score
CV Mean	99,93 %	99.87%	100%	99,93%
CV Std Dev	0,008%	0,017%	0,008%	0,008%
Test Set	99,92%	98,78%	99,92%	99,35%
CV-Test Gap	0,01%	1,09%	0,08%	0,59%
Stability	Very Stable	Very Stable	Very Stable	Very Stable
Consistency	Consistent	Acceptable	Consistent	Acceptable

Tabel 4.5 Algoritma Soft Voting

Parameter	Akurasi	Presisi	Recall	F1-Score
CV Mean	99,91 %	99.83%	99,99%	99,91%
CV Std Dev	0,010%	0,015%	0,006%	0,010%
Test Set	99,85%	97,76%	99,75%	98,74%
CV-Test Gap	0,06%	2,08%	0,25%	1,17%
Stability	Very Stable	Very Stable	Very Stable	Very Stable
Consistency	Consistent	Acceptable	Consistent	Acceptable

Tabel 4.6 Algoritma Hard Voting

Parameter	Akurasi	Presisi	Recall	F1-Score
CV Mean	99,85 %	99.70%	100%	99,85%
CV Std Dev	0,015%	0,026%	0,006%	0,015%
Test Set	99,76%	96,20%	99,87%	98,00%
CV-Test Gap	0,09%	3,50%	0,12%	1,85%
Stability	Very Stable	Very Stable	Very Stable	Very Stable
Consistency	Consistent	Acceptable	Consistent	Acceptable

Analisis konsistensi antara kinerja validasi silang dan kinerja set pengujian memberikan wawasan penting tentang kemampuan model. Random Forest menunjukkan gap CV-Test yang sangat minimal pada semua metrik: gap akurasi 0,01%, gap presisi 1,09%, gap recall 0,08%, dan gap F1-Score 0,59%. Ini menunjukkan bahwa performa model pada validasi silang sangat representatif terhadap performa aktual pada data pengujian yang tidak terlihat, menunjukkan model yang sangat baik tanpa overfitting. Secara perbandingan, model lain menunjukkan gap yang sedikit lebih besar khususnya pada Precision metric.

KNN memiliki Precision gap 7,53%, SVM 4,74%, Soft Voting 2,08%, dan Hard Voting 3,50% yang dapat dijelaskan oleh perbedaan distribusi antara Training Set (hasil SMOTE) dan Test Set (Original Distribution). Presisi yang sedikit lebih rendah pada set pengujian dibandingkan validasi silang adalah model yang diharapkan. Karena pada set pengujian, menghasilkan data yang tidak seimbang, sehingga ambang batas untuk prediksi positif perlu waktu lebih untuk pengujian menghindari bias yang berlebihan mengingat tingkat fraud yang rendah (5,88%).

Perbandingan model antar algoritma juga mengungkapkan karakteristik intrinsik dari paradigma pembelajaran masing-masing. Random Forest menunjukkan stabilitas tertinggi dengan standar deviasi secara konsisten <0,01%

pada semua metrik, ini mencerminkan sifat ensemble yang secara inheren mengurangi varian melalui bagging dan rata-rata di beberapa pohon keputusan. Metode ensemble lainnya (Soft Voting dan Hard Voting) juga menunjukkan stabilitas yang sangat baik (std dev 0,010-0,015%), memvalidasi manfaat teoritis dari pembelajaran ensemble dalam mengurangi prediksi berlebih.

ML berbasis instance seperti K-Nearest Neighbors, meskipun masih tergolong sangat stabil (std dev 0,023-0,047%), menunjukkan sedikit lebih banyak varian dibandingkan metode ensemble karena prediksi-nya lebih sensitif terhadap komposisi lingkungan lokal yang dapat bervariasi di berbagai pengujian. Support Vector Machine dengan std dev 0,008-0,038% menunjukkan stabilitas yang sangat baik, memanfaatkan optimalisasi prinsip margin maksimum yang menghasilkan batas keputusan yang konsisten di berbagai subset pelatihan.

Analisis cross-validation juga memvalidasi bahwa pilihan hyperparameter yang dilakukan dalam penelitian ini—seperti n_neighbors=5 untuk KNN, kernel='rbf' dengan C=1.0 untuk SVM, dan n_estimators=100 dengan max_depth=20 untuk Random Forest—menghasilkan model yang kuat dan tidak overfitted. Konsistensi antara validasi silang dan kinerja set pengujian, dikombinasikan dengan varian rendah di seluruh lipatan, menunjukkan bahwa hyperparameter berada dalam rentang optimal yang memungkinkan model untuk menangkap pola dasar yang sebenarnya tanpa mengingat kebisingan spesifik pelatihan. Tidak adanya overfitting yang signifikan sangat penting dalam deteksi penipuan.

BAB 5

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil dan pembahasan dapat disimpulkan beberapa hasil sebagai berikut:

a. Performa model ML SVM, RF, KNN dengan *voting classifier* dapat mendeteksi aktivitas kecurangan pada transaksi ATM di Bank Pembangunan Daerah Sulawesi Tenggara.

b. Tingkat akurasi dan metrik evaluasi dari model SVM, RF, KNN dengan *voting classifier* dalam mendeteksi kecurangan pada transaksi ATM menunjukkan nilai F1-Score yang paling baik adalah model algoritmik RF yakni 99% dari total data yang menjadi bahan penelitian sedangkan kurva roc menunjukkan hal yang signifikan dengan nilai 99%, mengungguli SVM (F1-Score 97%), KNN (F1-Score 95%), Ensemble Hard dan Soft Voting (F1-Score 98%). Performa RF dapat diatribusikan pada kemampuan ensemble internal-nya dalam menangkap pola non-linear yang kompleks dan interaksi features dalam konteks fraud.

c. Secara keseluruhan, performa KNN, SVM, RF dengan *soft* dan *hard* voting dalam deteksi transaksi fraud sangat ditentukan oleh kualitas data (khususnya penanganan class imbalance), pemilihan dan tuning algoritma, serta desain ensemble dan strategi evaluasi yang sensitif terhadap metrik seperti recall, F1-Score, dan ROC-AUC yang lebih relevan daripada akurasi saja pada kasus fraud. Literatur fraud detection terkini secara konsisten menunjukkan bahwa

d. kombinasi RF/SVM + oversampling (SMOTE/varian) + voting ensemble memberikan peningkatan nyata pada deteksi fraud dibanding model tunggal tanpa penyesuaian tersebut

e. Penerapan metode ensemble learning dengan SMOTE dapat meningkatkan performa model dibandingkan dengan model SVM, RF, KNN tanpa *voting classifier* secara individual.

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan saran yang dapat diajukan penulis sebagai berikut:

a. Penelitian ini berhasil mencapai akurasi tinggi yaitu 99% pada dataset periode September 2025, namun pengunaan data hanya dari data satu bulan saja dapat menimbulkan keterbatasan dalam menangkap pola fraud yang bersifat temporal sehingga penelitian selanjutnya disarankan mengunakkan dataset multi-periode minimal 6 – 12 bulan untuk menguji stabilitas dan konsistensi performa model terhadap variasi pola transaksi sepanjang tahun.

b. Hasil penelitian ini menggunakkan SMOTE dalam mensintesis data diperlukan ekplorasi alternatif seperti ADASYN atau kombinasi undersampling, oversampling untuk memvalidasi kekuatan model.

c. Penelitian ini belum mengekplorasi Teknik ensamble learning yang lebih *advanced* seperti Stacking atau Boosting yang terbukti efektif dalam berbagai deteksi fraud detection sehingga perlu dilakukan perbandingan dengan metode ensamble tersebut.

d. Dataset penelitian ini berasal dari satu cabang (Bank Sultra Sao-sao) yang mungkin memiliki karakteristik transaksi spesifik, sehingga generalisasi model perlu diuji pada data dari cabang lain untuk memastikan model tidak hanya efektif di salah satu cabang tertentu saja.

e. Penelitian ini belum mengeksplorasi penerapan *deep learning* seperti LSTM atau Autoencoder yang mampu menangkap pola temporal dan deteksi anomaly yang lebih rumit, sehingga penelitian selanjutnya dapat mengintegrasikan pendekatan hybrid antara machine learning dengan deep learning dalam mendeteksi fraud.

DAFTAR PUSTAKA

Aghware, F. O., Ojugo, A. A., Adigwe, W., Odiakaose, C. C., Ojei, E. O., Ashioba, N. C., Okpor, M. D., & Geteloma, V. O. (2024). *Enhancing the Random Forest Model via Synthetic Minority Oversampling Technique for Credit-Card Fraud Detection*.

Ahmed, K. H., Axelsson, S., Li, Y., & Sagheer, A. M. (2025). A credit card fraud detection approach based on ensemble machine learning classifier with hybrid data sampling. *Machine Learning with Applications*, *20*(May), 100675. https://doi.org/10.1016/j.mlwa.2025.100675

Ajay Kumar. (2024). Voting Classifier as a Balanced Framework for Fraud Detection in Imbalanced Credit Card Transactions. *Journal of Information Systems Engineering and Management*, *9*(4s), 2393–2410. https://doi.org/10.52783/jisem.v9i4s.12735

Andrade-Arenas, L., & Yactayo-Arias, C. (2025). Comparative Analysis of Machine Learning Models for Credit Card Fraud Detection Using SMOTE for Class Imbalance. *International Journal of Safety and Security Engineering*, *15*(5), 893–901. https://doi.org/10.18280/ijsse.150504

Astuti, F. D., & Lenti, F. N. (2021). Implementasi SMOTE untuk mengatasi Imbalance Class pada Klasifikasi Car Evolution menggunakan K-NN. *Jurnal JUPITER*, *13*(1), 89–98.

Basha, S. J., Madala, S. R., Vivek, K., Kumar, E. S., & Ammannamma, T. (2022). A Review on Imbalanced Data Classification Techniques. *2022 International Conference on Advanced Computing Technologies and Applications, ICACTA*

2022. https://doi.org/10.1109/ICACTA54488.2022.9753392

Cao-Van, K., Minh, T. C., Minh, L. G., Quyen, T. T. B., & Tan, H. M. (2024). Soft-Voting Ensemble Model: An Efficient Learning Approach for Predictive Prostate Cancer Risk. *Vietnam Journal of Computer Science*, *11*(4), 531–552. https://doi.org/10.1142/S2196888824500155

de Oliveira, G. P., Fonsêca, A., & Rodrigues, P. C. (2022). Diabetes diagnosis based on hard and soft voting classifiers combining statistical learning models. *Brazilian Journal of Biometrics*, *40*(4), 415–427. https://doi.org/10.28951/bjb.v40i4.605

Dede Kurniadi, Asri Indah Pertiwi, & Asri Mulyani. (2025). Ensemble Voting Classifier Berbasis Multi-Algoritma dan Metode SMOTE untuk Klasifikasi Penyakit Jantung. *Jurnal Nasional Teknik Elektro Dan Teknologi Informasi*, *14*(2), 145–153. https://doi.org/10.22146/jnteti.v14i2.17157

Dinata, R. kusuma, & Hasdina, N. (2020). *Machine Learning.pdf*.

Dong, Y., Xie, K., Bohan, Z., & Lin, L. (2021). A Machine Learning Model for Product Fraud Detection Based on SVM. *Proceedings - 2021 2nd International Conference on Education, Knowledge and Information Management, ICEKIM 2021*, 385–388. https://doi.org/10.1109/ICEKIM52309.2021.00091

Eldo, H., Ayuliana, Suryadi, D., Chrisnawati, G., & Judijanto, L. (2024). Penggunaan Algoritma Support Vector Machine (SVM) Untuk Deteksi Penipuan pada Transaksi Online. *Jurnal Minfo Polgan*, *13*, 1627–1632.

Fauzi, M. A., & Bours, P. (2020). Ensemble Method for Sexual Predators

Identification in Online Chats. *2020 8th International Workshop on Biometrics and Forensics, IWBF 2020 - Proceedings*, 1–6. https://doi.org/10.1109/IWBF49977.2020.9107945

Gnip, P., Vokorokos, L., & Drotár, P. (2021). Selective oversampling approach for strongly imbalanced data. *PeerJ Computer Science*, *7*, 1–22. https://doi.org/10.7717/PEERJ-CS.604

Hapsari, R. D., & Pambayun, K. G. (2023). ANCAMAN CYBERCRIME DI INDONESIA: Sebuah Tinjauan Pustaka Sistematis. *Jurnal Konstituen*, *5*(1), 1–17. https://doi.org/10.33701/jk.v5i1.3208

Hasanah, U., & Basarah, B. (2023). Transaksi Online Menurut Hukum Perjanjian Dikaitkan Dengan Pelindungan Konsumen Di Indonesia. *Jurnal Reehts Vinding: Media …*, *12*(2), 301–317.

Hasibuan, L. S., & Jannah, F. A. (2023). Deteksi Penipuan Kartu Kredit Menggunakan Support Vector Machine Dengan Optimasi Grid Search Dan Genetic Algorithm. *Building of Informatics, Technology and Science (BITS)*, *6*(1), 344–353. https://doi.org/10.47065/bits.v6i1.5355

Itoo, F., Meenakshi, & Singh, S. (2021). Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection. *International Journal of Information Technology (Singapore)*, *13*(4), 1503–1511. https://doi.org/10.1007/s41870-020-00430-y

Jauhari, M. I., Wirakusuma, M. P., Sidqi, A., Putra, I. G. N. R. A., Wijayanto, I., Rizal, A., & Hadiyoso, S. (2024). Implementation of Ensemble Machine Learning with Voting Classifier for Reliable Tuberculosis Detection Using

Chest X-ray Images with Imbalance Dataset. *Journal of Electronics, Electromedical Engineering, and Medical Informatics*, *6*(4), 543–548. https://doi.org/10.35882/jeeemi.v6i4.472

Lopez-Bernal, D., Balderas, D., Ponce, P., & Molina, A. (2021). Education 4.0: Teaching the basics of knn, lda and simple perceptron algorithms for binary classification problems. *Future Internet*, *13*(8). https://doi.org/10.3390/fi13080193

Madhurya, M. J., Gururaj, H. L., Soundarya, B. C., Vidyashree, K. P., & Rajendra, A. B. (2022). Exploratory analysis of credit card fraud detection using machine learning techniques. *Global Transitions Proceedings*, *3*(1), 31–37. https://doi.org/10.1016/j.gltp.2022.04.006

Margaret, M. (2023). *Cybercrime and its Impact on Nigeria ' s Digital Economy*.

Maulani, J., & Sari, M. (2023). Komparasi Metode K-Nearest Neighbor (Knn) Dengan Support Vector Machine (Svm) Terhadap Tingkat Akurasi Klasifikasi Kualitas Air. *Smart Comp: Jurnalnya Orang Pintar Komputer*, *12*(2), 430–435. https://doi.org/10.30591/smartcomp.v12i2.4205

Nur Avia Aminia Junaedy, & Nurul Asfiah. (2024). Hubungan antara AI, Machine Learning, Dan Implikasinya Terhadap Responsivitas Bisnis. *Jurnal Bisnis Inovatif Dan Digital*, *1*(3), 81–91. https://doi.org/10.61132/jubid.v1i3.189

Obasi, C., NNAkwuzie, D., Akobundu, C., Oketa, K., Richard-Nnabu, N., Azegba, O., Idris Yinka, A., Ifebude, B., & Bakpo, F. S. (2024). *Intelligent Authentication Agent Model for Detection of ATM Card Fraud in Nigeria*. *March*.

Osmond, A. B. (2025). *GNN Feature Engineering for Credit Card Fraud Detection : A Comprehensive Research Framework*. *08*(02), 232–247.

Pratama, M. D., Raharjo, A. B., & Purwitasari, D. (2023). ENSEMBLE OVERSAMPLING FOR FINANCIAL FRAUD CLASSIFICATION OF IMBALANCED DATA. *IPTEK The Journal of Techonology and Science*, *34*(2). https://doi.org/10.12962/j20882033.v34i3.17183

Purwaningsih, E., & Nurelasari, E. (2021). Penerapan K-Nearest Neighbor Untuk Klasifikasi Tingkat Kelulusan Pada Siswa. *Syntax : Jurnal Informatika*, *10*(01), 46–56. https://doi.org/10.35706/syji.v10i01.5173

Pushpita Anna Octaviani, Yuciana Wilandari, D. I. (2014). Penerapan Metode SVM Pada Data Akreditasi Sekolah Dasar Di Kabupaten Magelang. *Jurnal Gaussian*, *3*(8), 811–820.

Rahmadani, M., Andriani, S., & Elfina, R. (2023). Teknologi AI Dalam Meningkatkan Akurasi Sistem Pencarian Informasi Kesehatan. *Libria*, *15*(1), 89. https://doi.org/10.22373/21712

Rai, B., & Thapa, B. (2024). *LEEWAY IN THE DIGITAL SPACE : RISE OF CYBER CRIME , A CASE STUDY*. *3*, 9–18.

Ramadhani, M. A. T., Permata Sari, D., Sabilah, A. A., Tabitha, A. H., Rochmah, A., Saputra, A., Natasya, E., & Pratamah, D. A. (2025). Pemodelan Prediksi Nilai IQ Menggunakan Algoritma Machine Learning. *Jurnal Teknologi Dan Sistem Informasi Bisnis*, *7*(2), 262–267. https://doi.org/10.47233/jteksis.v7i2.1851

RB, A., & KR, S. K. (2021). Credit card fraud detection using artificial neural

network. *Global Transitions Proceedings*, *2*(1), 35–41. https://doi.org/10.1016/j.gltp.2021.01.006

Rochmawati, N., Zyen, A. K., Widiastuti, N. A., & Bill, T. N. I. (2025). *Comparison of Support Vector Machine (SVM) and Random Forest Algorithms in the Analysis of Social Media X User Sentiment Towards the TNI Bill*. *9*(5), 2854–2860.

Sarker, A., Yasmin, M. A., Rahman, M. A., Rashid, M. H. O., & Roy, B. R. (2024). On Credit Card Fraud Detection Using Machine Learning Techniques. *Journal of Computer and Communications*, *966 LNNS*(12), 1–11. https://doi.org/10.1007/978-981-97-2004-0_21

Sherazi, S. W. A., Bae, J. W., & Lee, J. Y. (2021). A soft voting ensemble classifier for early prediction and diagnosis of occurrences of major adverse cardiovascular events for STEMI and NSTEMI during 2-year follow-up in patients with acute coronary syndrome. *PLoS ONE*, *16*(6 June 2021), 1–20. https://doi.org/10.1371/journal.pone.0249338

Siringoringo, R. (2018). KLASIFIKASI DATA TIDAK SEIMBANG MENGGUNAKAN ALGORITMA SMOTE DAN k-NEAREST NEIGHBOR. *Jurnal ISD*, *3*(1), 44–49.

Soni, K. B., Chopade, M., & Vaghela, R. (2021). *Credit Card Fraud Detection Using Machine Learning Approach*. *4*(2), 71–76.

Suci Amaliah, Nusrang, M., & Aswi, A. (2022). Penerapan Metode Random Forest Untuk Klasifikasi Varian Minuman Kopi di Kedai Kopi Konijiwa Bantaeng. *VARIANSI: Journal of Statistics and Its Application on Teaching and*

Research, *4*(3), 121–127. https://doi.org/10.35580/variansiunm31

Sudin, A., Salmin, M., Fhadli, M., & ... (2023). Klasifikasi Kelayakan Air Minum Bagi Tubuh Manusia Menggunakan Metode Support Vektor Machine Dengan Backward Elimination. *Jurnal Jaringan Dan ...*, *3*(1), 87–95. https://doi.org/00.0000/jati

Syahbani, A. M., Firdaus, W., & Musodo, K. A. (2025). A Comparative Study of Data Mining Algorithms for Fraud Detection in Financial Transactions. *Sinkron*, *9*(2), 814–821. https://doi.org/10.33395/sinkron.v9i2.14645

Tanapanichkan, S., Kosolsombat, S., & Luangwiriya, T. (2024). Credit Card Fraud Detection Using Machine Learning. *International Conference on Cybernetics and Innovations, ICCI 2024*, *10*, 1628–1631. https://doi.org/10.1109/ICCI60780.2024.10532670

Uddin, S., Haque, I., Lu, H., Moni, M. A., & Gide, E. (2022). Comparative performance analysis of K-nearest neighbour (KNN) algorithm and its different variants for disease prediction. *Scientific Reports*, *12*(1), 1–11. https://doi.org/10.1038/s41598-022-10358-x

Vika Vitaloka Pramansah. (2022). Analisis Perbandingan Algoritma SVM Dan KNN Untuk Klasifikasi Anime Bergenre Drama. *Jurnal Informatika Dan Teknologi Komputer (J-ICOM)*, *3*(1), 49–55. https://doi.org/10.33059/j-icom.v3i1.4950

Wibisono, W. (2023). Preliminary Study on Corruption Case in the Indonesian Banking Sector: Overview of the Fraudster, Loss, and Fraud Modes. *Asia Pacific Fraud Journal*, *8*(1), 31. https://doi.org/10.21532/apfjournal.v8i1.263

Yazid, Y., & Fiananta, A. (2017). Mendeteksi Kecurangan Pada Transaksi Kartu Kredit Untuk Verifikasi Transaksi Menggunakan Metode Svm. *Indonesian Journal of Applied Informatics*, *1*(2), 61–66.

Zhang, S. (2020). Cost-sensitive KNN classification. *Neurocomputing*, *391*(xxxx), 234–242. https://doi.org/10.1016/j.neucom.2018.11.101

LAMPIRAN