Terjemahan artikel 10.22146/jnteti.v14i2.17410

Deteksi Transaksi Penipuan pada Sektor Perbankan Menggunakan *Ruled-Based Model* dan Pembelajaran Mesin

Cut Dinda Rizki Amirillah

Program Studi Ilmu Komputer, Fakultas Ilmu Komputer, Bina Nusantara University, Jakarta Barat, DKI Jakarta 11530, Indonesia

[Diserahkan: 18 November 2024, Direvisi: 22 Januari 2025, Diterima: 16 April 2025]
Penulis Korespondensi: Cut Dinda Rizki Amirillah (email: cut.amirillah@binus.ac.id)

INTISARI — Penelitian ini bertujuan untuk mengembangkan model deteksi penipuan yang efektif dalam transaksi perbankan menggunakan pendekatan *rule-based model* (RBM) dan algoritma pembelajaran mesin *isolation forest* (IF). Berdasarkan data Kementerian Komunikasi dan Informatika, terdapat lebih dari 405.000 kasus penipuan daring selama periode 2019–2022. Hal ini menunjukkan perlunya sistem deteksi penipuan yang andal untuk melindungi nasabah. Metode penelitian meliputi pengumpulan data transaksi perbankan ATM, *internet banking*, dan *mobile banking* selama empat bulan. Model RBM digunakan sebagai pendekatan awal yang mendeteksi pola transaksi mencurigakan berdasarkan aturan yang ditetapkan. Akan tetapi, model ini memiliki keterbatasan dalam mendeteksi transaksi yang tidak ditetapkan dalam aturan. Untuk mengatasi kekurangan ini, penelitian ini mengimplementasikan IF, sebuah model pembelajaran takterbimbing yang efektif untuk mendeteksi anomali menggunakan teknik *isolation tree* (iTree) untuk mengidentifikasi transaksi mencurigakan. Hasil penelitian menunjukkan bahwa model IF dapat mendeteksi pola anomali yang tidak dapat dideteksi oleh RBM, sehingga meningkatkan akurasi identifikasi transaksi penipuan. Data presisi sebesar 99% menunjukkan bahwa prediksi anomali yang dilakukan model memang merupakan anomali, sedangkan nilai *recall* sebesar 1,0 menunjukkan bahwa model berhasil mengidentifikasi semua anomali dalam *dataset*. Oleh karena itu, dapat disimpulkan bahwa kombinasi RBM dan IF menawarkan pendekatan yang komprehensif dalam upaya deteksi penipuan di sektor perbankan. Kemampuan IF untuk mendeteksi anomali dengan lebih dinamis dan akurat dapat mengurangi kerugian akibat penipuan di industri tersebut.

KATA KUNCI — Pembelajaran Mesin, *Isolation Forest* (IF), *Rule-Based Model* (RBM), Sektor Perbankan.

I. PENDAHULUAN

Menurut Kementerian Komunikasi dan Informatika, dari tahun 2019 hingga 2022 terdapat sekitar 486.000 kasus penipuan yang terdokumentasikan. Di antara kasus-kasus tersebut, 405.000 laporan berupa penipuan daring, sehingga menjadikan penipuan ini sebagai penipuan yang paling umum terjadi. Penting untuk dicatat bahwa penipuan skala kecil merupakan akar penipuan yang lebih besar dengan dampak yang lebih luas, misalnya penggelapan dana skala besar hingga penyalahgunaan kredit debitur yang terbukti dapat merugikan bank [1]. Di Indonesia, regulator, seperti Bank Indonesia dan Otoritas Jasa Keuangan, telah menetapkan pedoman penerapan strategi antipenipuan bagi bank. Peraturan yang diuraikan dalam Peraturan Otoritas Jasa Keuangan (POJK) Nomor 39/POJK.03/2019 [2] dan Bank Indonesia Nomor 23/6/PBI/2021 [3] ini secara khusus ditujukan kepada penyedia layanan pembayaran. Penyedia layanan keuangan diwajibkan untuk mengadopsi sistem antipenipuan, dengan sistem deteksi penipuan sebagai komponen utama. Sistem ini menggabungkan *rule-based model* (RBM) yang berfungsi sebagai filter data sebelum diproses. Meskipun metode konvensional masih dapat digunakan, metode ini dianggap kurang efektif dalam mendeteksi transaksi skala besar di sektor perbankan [4].

Penipuan merupakan istilah komprehensif yang merujuk pada tindakan yang bertujuan untuk memperoleh keuntungan finansial menggunakan cara ilegal dan melakukan penipuan di berbagai sektor, termasuk asuransi, perbankan, perpajakan, dan ranah korporat [5]. Segitiga penipuan, sebuah model yang menggambarkan kondisi-kondisi yang dapat meningkatkan kemungkinan terjadinya penipuan, telah dikonseptualisasikan oleh para peneliti [6] dan Association of Certified Fraud Examiners (ACFE) [7]. Tekanan merupakan situasi ketika individu mulai termotivasi untuk terlibat dalam penipuan. Peluang adalah keadaan yang dimanfaatkan oleh penjahat untuk melakukan penipuan, sedangkan rasionalisasi adalah tahap ketika pelaku meyakinkan diri bahwa tindakan tesrsebut dibenarkan, sehingga mengurangi perasaan bersalah. Saat ini, bank memiliki sistem deteksi penipuan untuk mengidentifikasi data yang mencurigakan berdasarkan RBM. RBM merupakan pendekatan yang digunakan untuk mendeteksi transaksi penipuan [8]. Setiap aturan dilengkapi dengan ambang batas yang dapat disesuaikan untuk memenuhi persyaratan bank. Kategori RBM dan ambang batas untuk mengidentifikasi transaksi yang mencurigakan diuraikan dalam Tabel I.

Perilaku keuangan dirancang untuk mengidentifikasi pola transaksi keuangan yang terjadi berulang kali dalam periode singkat dan dengan jumlah yang tidak biasa. Perilaku pengguna adalah aturan yang dirancang untuk mendeteksi aktivitas *login* berulang dan pemeriksaan saldo dalam interval waktu yang dekat. Beberapa akun dirancang untuk mengidentifikasi pola *1-to-many*, saat satu akun mengirim transaksi ke beberapa akun secara bersamaan. Penerapan RBM memiliki keuntungan signifikan dalam mendeteksi transaksi penipuan. Namun, RBM memiliki kelemahan, yaitu transaksi dengan anomali di luar ambang batas yang telah ditetapkan tidak dapat diidentifikasi oleh aplikasi sistem deteksi penipuan. Oleh karena itu, metode pembelajaran mesin diperlukan untuk memprediksi transaksi penipuan [9]. Dibandingkan dengan RBM konvensional, pendekatan pembelajaran mesin dapat lebih efektif dalam

TABEL I
RULE-BASED MODEL (RBM)

No	Kategori	Ambang
1	Perilaku keuangan	Jumlah total, waktu jangkauan, frekuensi.
2	Perilaku pengguna	Frekuensi *login*, upaya memeriksa saldo.
3	Beberapa akun	Transaksi *1-to-many*, jumlah akun tujuan.

memproses *dataset* skala besar. Maka, pembelajaran mesin perlu diterapkan. Dalam mengembangkan model pembelajaran mesin untuk deteksi penipuan, model-model ini umumnya menggunakan klasifikasi. Model klasifikasi berfungsi untuk membedakan transaksi sebagai penipuan atau bukan penipuan, sehingga memberikan cara yang efektif untuk menentukan metode deteksi penipuan keuangan yang sesuai [10].

Pembelajaran mesin, salah satu aspek kecerdasan buatan, berfokus pada pengembangan algoritma dan model statistik yang memungkinkan komputer untuk belajar dari data dan membuat prediksi atau keputusan berdasarkan pola yang teridentifikasi [11]. Pembelajaran mesin berfungsi sebagai teknik analitis yang mampu mengungkap pola tanpa panduan manual dari ahli [12]. Dalam industri perbankan, pembelajaran mesin dapat meningkatkan deteksi penipuan dengan menganalisis data skala besar untuk mengidentifikasi pola yang tidak dapat diidentifikasi oleh RBM konvensional. Penelitian ini menggunakan pembelajaran takterbimbing (*unsupervised learning*), model pembelajaran mesin yang andal dalam mendeteksi transaksi anomali, sehingga dapat mengungkap pola dan anomali yang menunjukkan perilaku penipuan. Hal ini memungkinkan pendeteksian dan pencegahan penipuan secara *real-time*, sehingga meminimalkan peringatan palsu dan meningkatkan keamanan [13].

Isolation forest (IF), yang merupakan metode pembelajaran takterbimbing, terdiri atas kumpulan *isolation trees* (iTrees) yang berasal dari *dataset* untuk mendeteksi anomali dalam mengidentifikasi transaksi penipuan [14]. Deteksi anomali dengan IF terdiri atas dua tahap. Tahap awal adalah tahap pelatihan, yaitu tahap membangun iTrees menggunakan subsampel *dataset* pelatihan. Lalu, tahap pengujian meliputi penetapan contoh uji ke iTrees, sehingga menghasilkan nilai anomali untuk setiap contoh [15].

Urgensi penelitian ini terletak pada maraknya kasus penipuan yang makin kompleks dan secara signifikan berdampak pada stabilitas sektor perbankan. Dengan mengadopsi metode pembelajaran mesin, khususnya yang berbasis pembelajaran takterbimbing, diharapkan deteksi penipuan dapat dilakukan secara lebih efektif dan tepat waktu, sehingga dapat meminimalkan kerugian finansial yang lebih besar dan menjaga integritas sistem perbankan.

Penelitian sebelumnya berfokus pada deteksi penipuan menggunakan RBM dan metode tradisional lainnya [5]. Penggunaan metode tersebut terbukti cukup efisien dalam mengidentifikasi anomali tertentu, tetapi memiliki keterbatasan dalam hal skalabilitas dan fleksibilitas. Sementara itu, penelitian lain mengeksplorasi pendekatan pembelajaran mesin, khususnya model klasifikasi, untuk meningkatkan akurasi deteksi dan mengidentifikasi aktivitas penipuan secara dinamis [6]. Namun, penelitian ini sering kali menitikberatkan pada pembelajaran terbimbing (*supervised learning*), yang memerlukan *dataset* berlabel. Hal ini merupakan tantangan tersendiri mengingat *dataset* berlabel tidak mudah diperoleh dalam skenario dunia nyata.

Studi ini mengatasi kesenjangan tersebut dengan mengadopsi pendekatan pembelajaran takterbimbing, khususnya IF, untuk meningkatkan deteksi penipuan dalam transaksi perbankan. Metode IF telah menunjukkan hasil yang menjanjikan dalam mendeteksi anomali dengan menggunakan struktur iTrees yang unik untuk mengisolasi *outlier* dari data secara efisien [7]. Tidak seperti model terbimbing, metode IF tidak memerlukan data berlabel, sehingga sangat sesuai untuk *dataset* perbankan dengan klasifikasi awal yang minimal.

Kebaruan penelitian ini terletak pada pengintegrasian model pembelajaran takterbimbing dengan RBM tradisional untuk mengembangkan kerangka kerja gabungan yang mampu mengatasi keterbatasan masing-masing pendekatan. Dengan memanfaatkan kekuatan pembelajaran mesin, penelitian ini berkontribusi pada pengembangan sistem deteksi penipuan yang dapat diskalakan, adaptif, tangguh, dan dapat disesuaikan dengan sifat dinamis transaksi keuangan.

Pentingnya penelitian ini terletak pada potensinya untuk mengurangi kerugian finansial dan memperkuat stabilitas sektor perbankan. Seiring dengan makin kompleksnya kasus penipuan dan dampaknya, penerapan sistem deteksi canggih sangat penting untuk melindungi lembaga keuangan dan meningkatkan kepercayaan publik. Selain itu, penelitian ini memberikan *roadmap* bagi penyedia layanan keuangan untuk beralih dari model deteksi konvensional ke solusi berbasis kecerdasan buatan (*artificial intelligence*, AI), sehingga memastikan pencegahan penipuan secara *real-time* dan meminimalkan kesalahan positif.

II. PENELITIAN TERKAIT

Lanskap perbankan saat ini dan penerapan deteksi penipuan sangat penting untuk menjaga keamanan transaksi keuangan [16]. Pada intinya, sistem ini bergantung pada pendekatan RBM yang setiap aturannya memiliki ambang batas, yaitu parameter yang diatur secara cermat agar selaras dengan toleransi risiko dan persyaratan khusus lembaga perbankan. Aturan-aturan ini bertindak seperti "penjaga gerbang" yang selalu waspada, yang secara sistematis menganalisis data yang masuk untuk mengidentifikasi dan menandai transaksi yang menunjukkan karakteristik aktivitas penipuan. Sifat terstruktur yang dimiliki RBM memastikan respons yang cepat terhadap potensi ancaman guna meningkatkan keamanan transaksi keuangan secara keseluruhan [17]. Meskipun efektif, RBM memiliki keterbatasan yang melekat, terutama kekakuannya, yang berarti bahwa transaksi dengan anomali di luar ambang batas yang telah ditentukan sebelumnya dapat lolos dari deteksi. Keterbatasan ini memerlukan solusi yang lebih adaptif dan canggih, yang mengarah pada integrasi pembelajaran mesin ke dalam deteksi penipuan.

Pembelajaran mesin memperkenalkan paradigma yang dinamis dan berorientasi pada pembelajaran, sehingga memungkinkan sistem untuk berevolusi dan beradaptasi dengan pola yang terus berubah dalam transaksi keuangan [18]. Penerapan model pembelajaran mesin memungkinkan sistem deteksi penipuan untuk memprediksi dan mengidentifikasi aktivitas penipuan yang mungkin luput dideteksi oleh RBM tradisional. Model pembelajaran mesin untuk deteksi penipuan memiliki dua kategori utama, yaitu model klasifikasi dan regresi [19]. Model klasifikasi unggul dalam membedakan transaksi sebagai penipuan atau bukan penipuan, menawarkan alat yang ampuh untuk membedakan metode yang efektif dalam lanskap deteksi penipuan keuangan [20]. Di sisi lain, model regresi digunakan untuk mengidentifikasi korelasi

antara variabel-variabel yang dapat berkontribusi pada transaksi yang diklasifikasikan sebagai penipuan.

Penggunaan teknik pembelajaran mesin tidak hanya meningkatkan efektivitas sistem deteksi penipuan secara keseluruhan, tetapi juga membuatnya dapat beradaptasi dengan pola aktivitas penipuan yang rumit dan terus berkembang [21]. Evolusi lanskap keuangan yang berkelanjutan menekankan pentingnya hubungan simbiosis antara RBM dan kemampuan IF pembelajaran mesin dalam memperkuat pertahanan terhadap ancaman penipuan keuangan yang terus-menerus. Dengan mengadopsi pendekatan gabungan ini, institusi menempatkan diri di garis terdepan dalam hal inovasi dan ketahanan guna menghadapi lanskap ancaman yang terus berkembang.

A. RULE-BASED MODEL

Sebagaimana dinyatakan pada penelitian sebelumnya, penipuan perlu diburu dan dideteksi secara aktif sedini mungkin [9]. Hal ini menjadi makin penting ketika metode terbimbing diterapkan pada deteksi penipuan. Salah satu metode yang dinilai sesuai adalah RBM, yang bekerja dengan mencocokkan setiap data dengan serangkaian indikator yang telah ditentukan sebelumnya. Penelitian ini berfokus pada pendeteksian kasus penipuan yang terjadi di jaringan telekomunikasi dan pengidentifikasian anomali pada proses klaim asuransi kesehatan atau memperingatkan terjadinya penipuan pada kredit konsumen. Pada proses pelatihannya, RBM tidak hanya melibatkan fitur numerik tradisional, tetapi juga fitur tekstual yang diekstraksi dari deskripsi melalui algoritma pemrosesan teks seperti alokasi Dirichlet laten.

Penelitian RBM lainnya mendeteksi transaksi kartu kredit yang tidak lazim dengan menggunakan metode *anomalous pattern and transaction inspection* (APATE), yang merupakan pendekatan baru untuk mendeteksi penipuan transaksi kartu kredit di toko daring [8]. Pendekatan tersebut menggabungkan dua hal berikut: 1) fitur intrinsik yang diperoleh dari karakteristik transaksi masuk dan riwayat pengeluaran pelanggan dengan menggunakan basis *recency–frequency–monetary* (RFM); dan 2) fitur berbasis jaringan dengan memanfaatkan jaringan pemegang kartu kredit dan pedagang untuk menghasilkan skor kecurigaan yang bergantung pada waktu setiap objek pada jaringan tersebut. Hasil penelitian menunjukkan bahwa dalam konteks yang sama, fitur intrinsik dan berbasis jaringan saling terkait erat. Kombinasi kedua jenis fitur ini menghasilkan model dengan kinerja terbaik dengan skor *area under the curve* (AUC) yang melebihi 0,98. Dari kedua penelitian tersebut, dapat disimpulkan bahwa RBM merupakan metode yang cocok untuk mendeteksi transaksi tidak lazim dengan menetapkan ambang batas yang dapat diatur oleh pengguna. Namun, dalam dekade terakhir, metode deteksi juga dapat dilakukan menggunakan pembelajaran mesin.

B. PEMBELAJARAN MESIN

Pada penelitian sebelumnya yang menggunakan model pembelajaran mesin, terdapat beberapa faktor yang memengaruhi kinerja IF dalam mendeteksi transaksi penipuan pada kanal kartu kredit [22]. Terdapat empat skenario eksperimen: analisis pengaruh rasio pemisahan (*split ratio*) pada data validasi, dampak pemilihan fitur, pengaruh jumlah data penipuan dalam set pelatihan, dan penyesuaian nilai hiperparameter [10]. Pernyataan tersebut menguraikan studi penelitian yang memanfaatkan model pembelajaran mesin, khususnya IF, untuk mendeteksi transaksi penipuan di sektor perbankan. Penelitian ini bertujuan untuk memahami dan mengevaluasi faktor-faktor yang memengaruhi kinerja model. Secara keseluruhan, penelitian ini bertujuan untuk memberikan wawasan tentang konfigurasi dan kondisi optimal bagi IF untuk meningkatkan efektivitasnya guna mengidentifikasi transaksi penipuan pada kartu kredit [23].

Penelitian lain telah menerapkan IF untuk mendeteksi anomali dan kejadian langka lainnya, seperti penipuan. Hasil penelitian menunjukkan bahwa pengaturan IF dapat secara signifikan meningkatkan metrik klasifikasi tradisional, seperti AUC, serta metrik tidak konvensional yang mungkin relevan bagi bisnis dengan sumber daya terbatas [24]. Perbandingan menggunakan pendekatan pengklasteran menunjukkan dampak yang serupa, menggambarkan bahwa kedua opsi tersebut sama-sama bermanfaat dalam mengeksplorasi deteksi anomali. Selain itu, hasil IF berpotensi mempermudah penafsiran di seluruh *dataset*. Secara keseluruhan, makalah ini menyoroti efektivitas IF dalam mendeteksi anomali, terutama dalam kasus penipuan, dan menekankan potensi keuntungannya, termasuk metrik klasifikasi yang lebih baik dan kemudahan interpretasi di berbagai *dataset* [25].

III. METODOLOGI

Kajian pustaka dilakukan dengan mengeksplorasi berbagai sumber yang membahas deteksi kecurangan. Selain itu, penelitian ini juga mengkaji penelitian terdahulu yang relevan. Dua pendekatan digunakan dalam mendeteksi transaksi kecurangan. Pendekatan pertama menggunakan RBM [8], sedangkan pendekatan kedua menggunakan metode IF pembelajaran mesin [24].

Pendekatan pertama, yang menggunakan RBM untuk mengidentifikasi penipuan dalam transaksi perbankan, mengandalkan aturan guna mengenali pola yang mencurigakan atau tidak biasa. Meskipun demikian, pendekatan ini memiliki keterbatasan karena hanya mampu mendeteksi transaksi mencurigakan yang telah ditetapkan dalam aturan. Oleh karena itu, diperlukan pendekatan kedua menggunakan IF [25].

Penelitian diawali dengan mengumpulkan *dataset* kegiatan perbankan selama kurun waktu empat bulan. Metode pertama yang diterapkan adalah RBM. Pada metode ini, logika RBM digunakan untuk mendeteksi pola transaksi. Metode kedua adalah IF melalui beberapa tahapan prapemrosesan data, meliputi pembersihan, pengolahan, dan persiapan data untuk penggunaan dalam model [26]. Selanjutnya, proses IF dilakukan dengan melatih model menggunakan *dataset* dan data pelatihan untuk mendeteksi pola anomali pada data. Hasil dari proses IF kemudian dievaluasi dan dianalisis untuk mengidentifikasi transaksi yang diduga sebagai kecurangan.

Langkah selanjutnya melibatkan analisis mendalam terhadap kecurangan yang terdeteksi. Proses analisis data perbankan diawali dengan pengumpulan *dataset* yang mencakup aktivitas perbankan selama periode empat bulan. *Dataset* ini menjadi dasar untuk membangun dua model utama, yaitu RBM dan IF.

Pada tahap pengembangan RBM, *dataset* diolah menggunakan logika *rule-base*, sehingga menghasilkan keluaran yang disebut hasil *rule-base*. Sementara itu, pada tahap pengembangan IF, data melewati proses prapemrosesan yang meliputi pembersihan, pengolahan, dan penyiapan data. Setelah data siap, algoritma IF diaplikasikan untuk mengolah *dataset*, sehingga didapatkan hasil IF. Selanjutnya, hasil kedua model, yaitu hasil *rule-base* dan hasil IF, digabungkan untuk membuat model akhir yang disebut kombinasi RBM + IF. Model gabungan ini selanjutnya dievaluasi untuk mengetahui

TABEL II
STRUKTUR *DATASET*

No	Kategori	Deskripsi	Nilai
1	*trkey*	Nomor referensi	341505001
2	*accountIssuer*	Peneribit nomor akun	1001568667
3	*accountDestination*	Nomor akun tujuan	1002158333
4	*trtime*	Tanggal dan waktu transaksi	2023-04-22 18:44:50.
5	*merchant*	Kanal transaksi	6410
6	*amount*	Nominal transaksi	90000000
7	*trtype*	Jenis transaksi	6011
8	*trdesc*	Deskripsi transakasi	BI-FAST
9	*financial*	Bendera keuangan	Y
10	*trdescdetail*	Detail transaksi	BI-FAST *Posting*
11	*responsecode*	Respons transaksi (sukses/gagal)	0
12	*responseaction*	Tindakan respons	Transaksi berhasil
13	*merchantdesc*	Deskripsi kanal	*Mobile Banking*
14	*destinationbank*	Bank tujuan	ZYZ
15	*issuerbank*	Bank penerbit	XYZ
16	*acqbank*	Bank yang mengakuisisi	XYX
17	*scenario*	Klasifikasi penipuan transaksi (penipuan/normal)	1TOMANY
18	*class*	Nomor referensi	1 / -1

kinerja dan validitasnya. Berdasarkan hasil evaluasi, hasil akhir model disajikan sebagai keluaran utama.

Proses ini didesain untuk meningkatkan akurasi dan efisiensi dalam menganalisis data aktivitas perbankan dengan menggunakan kelebihan setiap pendekatan, yaitu logika *rule-base* dan deteksi anomali menggunakan IF.

A. DATASET

Penelitian ini menggunakan *dataset* transaksi perbankan selama empat bulan. Data tersebut diekstrak dari basis data *mirroring* yang disediakan oleh bank, yang terdiri atas data transaksi pada kanal daring seperti ATM, *internet banking*, dan *mobile banking*. Data kemudian difilter ke dalam tabel transaksi yang relevan guna menganalisis data transaksi bank. Populasi data dalam penelitian ini mencakup transaksi dari 19 April 2023 hingga 31 Agustus 2023, dengan jumlah 2.968.228 baris, berdasarkan kriteria berikut:

1. dari 29 kolom data master, hanya 17 kolom yang digunakan pada penelitian ini;
2. hanya data transaksi keuangan yang digunakan; data nonkeuangan, seperti informasi saldo, aktivitas *login*, *logout*, atau perubahan profil, tidak disertakan;
3. hanya transaksi dengan status respons berhasil yang digunakan; data dengan respons gagal, seperti *timeout* atau saldo tidak mencukupi, tidak disertakan dalam penelitian;
4. data transaksi dilakukan melalui kanal daring, yaitu ATM, *internet banking*, dan *mobile banking*.

Pemilihan fitur data transaksi pada *dataset* kemudian dilakukan berdasarkan data tersebut. Hasil pemilihan fitur data ini menghasilkan 18 fitur data transaksi dan 1 fitur kelas, sebagai hasil klasifikasi transaksi yang terindikasi sebagai kecurangan. Fitur secara detail dapat dilihat pada Tabel II.

B. RULE-BASED MODEL

Metode RBM menggunakan seperangkat aturan atau syarat yang telah ditetapkan sebelumnya ketika mengidentifikasi pola yang mengindikasikan penipuan transaksi perbankan [8]. Guna mengidentifikasi transaksi yang mencurigakan dengan cepat dan efisien, proses deteksi penipuan berdasarkan RBM terdiri atas beberapa langkah utama [9]. Sumber data yang dikumpulkan dari berbagai kanal disimpan dalam basis data *mirroring* yang disiapkan dalam mode *real-time*. Mesin logika dengan Java Spring Boot menerapkan aturan yang telah ditetapkan oleh bank sebelumnya, dengan setiap aturan memiliki ambang batas untuk menentukan transaksi mencurigakan. Ambang batas ini bersifat dinamis, yang memungkinkan pengguna bank untuk menyesuaikannya sesuai dengan tren penipuan saat ini atau sesuai dengan kebutuhan bisnis. Aturan dirancang dengan mempertimbangkan pola penipuan umum. Berikut ini adalah aturan dan ambang batas yang diterapkan dalam penelitian ini.

1. Perilaku keuangan memiliki tiga parameter utama sebagai ambang batas, yaitu jumlah, frekuensi, dan interval waktu. Ambang batas interval waktu ditetapkan selama 1 menit, frekuensi 5 kali transaksi, dan ambang batas nominal sebesar Rp15.000.000. Dengan demikian, transaksi yang sama dengan atau melebihi Rp15.000.000, atau terdapat lebih dari 5 kali transaksi berulang dalam interval 1 menit, akan memicu skenario perilaku keuangan.
2. Perilaku pengguna dirancang dengan ambang batas percobaan *login* mencurigakan ditetapkan sebanyak 4 kali dalam interval 1 menit. Aturan ini memungkinkan model untuk secara efektif menangkap perilaku pengguna yang mencurigakan.
3. Beberapa akun dirancang untuk mengidentifikasi pola *1-to-many*. Dengan menetapkan ambang batas 5 akun penerima dalam interval 1 menit, upaya penipuan yang melibatkan transfer dana yang tidak biasa dapat dideteksi.

C. PEMBELAJARAN MESIN

Pertama-tama, *library* yang diperlukan diimpor, termasuk Pandas dan NumPy untuk pemrosesan data, Matplotlib dan Seaborn untuk visualisasi data, psycopg2 dan SQLAlchemy untuk koneksi SQL, dan ColumnTransformer untuk prapemrosesan fitur menggunakan teknik seperti BinaryEncoder, StandardScaler, dan OneHotEncoder.

1) PENENTUAN *OUTLIER*

Fungsi *outlier* digunakan untuk menghitung *outlier* dari suatu *dataset* [14]. Fungsi ini menghitung kuartil pertama (q1),

kuartil kedua (q2), dan kuartil ketiga (q3). Kemudian, digunakan rentang interkuartil (*interquartile* range, IQR) untuk menghitung batas bawah (*min_IQR*) dan batas atas (*max_IQR*) untuk menentukan *outlier*. Fungsi ini mengiterasi setiap elemen *dataset* untuk memeriksa nilai yang termasuk *outlier* dan yang bukan. Hasilnya ditampilkan dalam bentuk nama kolom, batas bawah, jumlah *outlier* bawah, jumlah *outlier* atas, dan daftar *outlier*.

2) PENENTUAN BATAS NORMAL

Batas "normal" digunakan untuk mengidentifikasi distribusi normal suatu variabel. Hasil pengujian dicetak bersama dengan hipotesis nol (H0) dan hipotesis alternatif (Ha) [27]. Jika nilai-*p* dari uji normalitas kurang dari atau sama dengan 0,05, maka hipotesis nol (transaksi normal) ditolak.

3) PENGUMPULAN DAN PERSIAPAN DATA

Fungsi "data_collected" mencetak informasi tentang data yang dikumpulkan, termasuk tanggal mulai, tanggal berakhir, dan jumlah titik data. Fungsi "data_prep" menyiapkan data dengan melakukan beberapa transformasi, seperti menghapus duplikat, mengubah tipe data, dan mengekstrak informasi tambahan dari kolom waktu.

Langkah persiapan untuk membangun dan melatih IF meliputi pemuatan data dari dua berkas CSV yang berbeda ke dalam kerangka data. Prapemrosesan meliputi pengisian nilai yang hilang di kolom "accountDestination" dengan string "na." Setelah itu, baris dengan nilai yang cocok dengan pola regex [A-Z+] di kolom "accountDestination" dihapus dari kerangka data. Fungsi "drop_exclude()" kemudian digunakan untuk mengecualikan baris dengan nilai di kolom "merchant" yang sudah disertakan dalam daftar dan fungsi "modify_trx_amount()" digunakan untuk mengubah nilai di kolom "amount" menurut kondisi tertentu. Langkah terakhir menyiapkan data menggunakan fungsi "data_prep()," yang mengubah tipe data dan mengekstrak informasi tambahan dari kolom "time".

4) *PIPELINE*

Pipeline terdiri atas dua langkah, yaitu *preprocessor* untuk mentransformasikan data dan "clf_iso" untuk menetapkan IF sebagai pengklasifikasi. Pada langkah pertama alur kerja, semua *transformer* yang ditetapkan sebelumnya dalam *preprocessor* diterapkan ke data masukan sebelum model dilatih. *Transformer* tersebut antara lain OneHotEncoder, BinaryEncoder, StandardScaler, dan TfidfVectorizer. Setelah melalui pemrosesan dengan *transformer*, data siap diproses oleh model. Pada langkah berikutnya, IF dibangun dengan *hyperparameter* yang telah ditetapkan sebelumnya. Nilai *n_estimators* ditetapkan sebesar 100 untuk menentukan jumlah pohon yang akan dibangun dalam ensambel, nilai *contamination* sebesar 0,01 untuk mengendalikan proporsi *outlier* yang diharapkan dalam data, dan *random_state* sebesar 42 untuk menetapkan nilai inisialisasi acak, yang penting untuk reproduktifitas hasil. Setelah membuat alur kerja, "model.fit(df[relevant_features])" digunakan untuk melatih model pada data masukan. Data yang digunakan untuk pelatihan merupakan bagian dari kerangka data "df" yang hanya terdiri atas kolom-kolom yang dianggap relevan untuk pelatihan model, sebagaimana ditentukan dalam variabel *relevance_features*. Setelah model dilatih, dilakukan prediksi pada data yang sama untuk mengidentifikasi keberadaan *outlier* pada setiap baris data. Selanjutnya, hasil prediksi disimpan dalam kolom baru bernama "ai_behavior" dalam kerangka data "df." Oleh karena itu, setiap baris data diberi label normal (1) atau abnormal (-1) berdasarkan prediksi model.

TABEL III
PERBANDINGAN ANTARA NORMAL DAN PENIPUAN

Prediksi	RBM	IF	RBM + IF
Normal	2.938.545	2.730.130	2.966.473
Penipuan	29.683	208.415	1.755

IV. HASIL DAN PEMBAHASAN

A. DATASET

Dari *dataset* yang dikumpulkan selama rentang waktu empat bulan dari kanal daring ATM, *mobile banking*, dan *internet banking*, model pembelajaran mesin memprediksi 2.938.545 transaksi sebagai transaksi normal dan 29.683 transaksi sebagai transaksi penipuan. Di sisi lain, RBM memprediksi 2.730.130 transaksi sebagai transaksi normal dan 208.415 transaksi sebagai transaksi penipuan. Kombinasi metode pembelajaran mesin dan RBM memprediksi 2.966.473 transaksi sebagai transaksi normal dan 1.755 transaksi sebagai transaksi penipuan. Tabel III menunjukkan perbandingan data kategori normal dan penipuan.

B. METODE EVALUASI

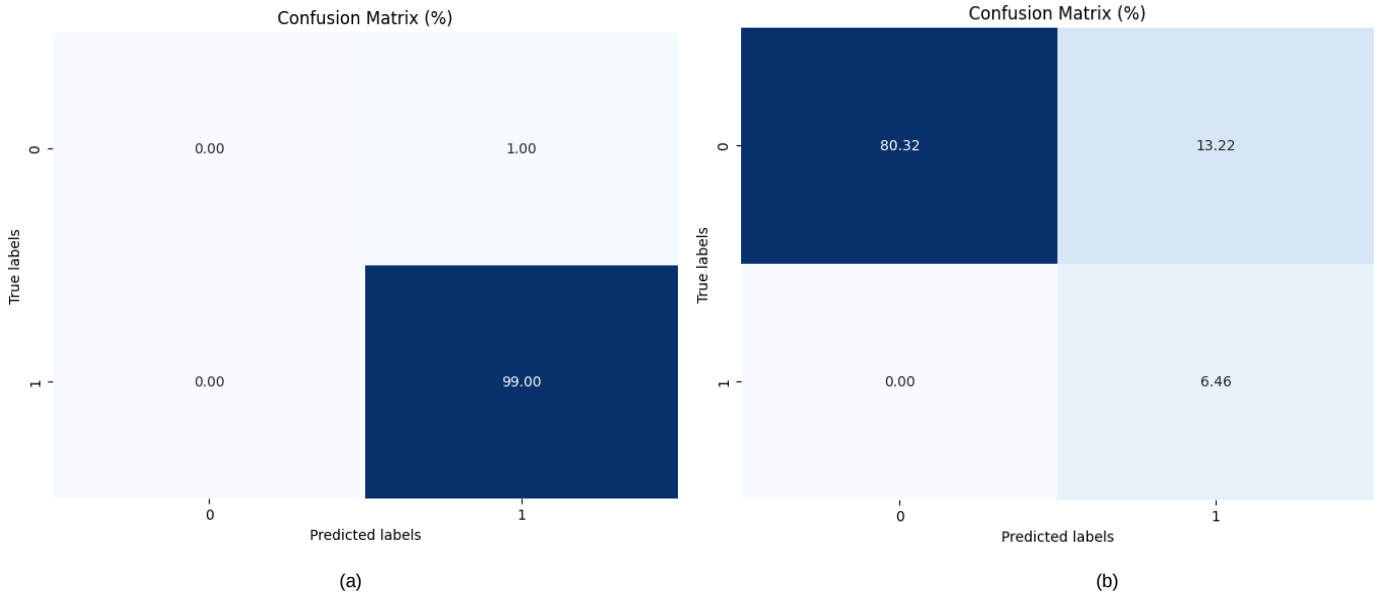
Penelitian ini menggunakan *confusion matrix* untuk mengevaluasi kinerja model. Akurasi dan presisi prediksi dapat ditentukan dengan membandingkan jumlah observasi yang diklasifikasikan dengan benar dan salah. Data ini kemudian digunakan untuk menghitung metrik, termasuk akurasi, presisi, *recall*, dan *F*1-*score*, dengan menggunakan rumus yang umum digunakan, termasuk dari penelitian sebelumnya [20]. Penjelasan rumus ini disajikan sebagai berikut.

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

True positive (*TP*) menunjukkan jumlah sampel positif yang diprediksi dengan benar oleh model. Jumlah sampel negatif yang diprediksi secara salah oleh model sebagai sampel positif dikenal sebagai *false positive* (*FP*), sedangkan *false negative* (*FN*) adalah jumlah sampel positif yang secara keliru diidentifikasi oleh model sebagai negatif. *True negative* (*TN*) adalah jumlah sampel negatif yang diidentifikasi dengan benar oleh model sebagai negatif [15].

C. HASIL ANALISIS

Berdasarkan Gambar 1, data presisi sebesar 99% menunjukkan bahwa prediksi anomali model memang merupakan anomali, sedangkan nilai *recall* sebesar 1,0 menunjukkan bahwa model berhasil mengidentifikasi semua anomali dalam *dataset*. Hasil evaluasi RBM ditunjukkan pada Gambar 1(b). Model menghasilkan akurasi sebesar 86,78%, yang menunjukkan tingkat kesesuaian antara prediksi yang benar dan total sampel. Namun demikian, presisi yang rendah, sebesar 32,83%, menunjukkan bahwa hanya sebagian kecil prediksi positif yang benar dan *recall* yang tinggi, sebesar 100%, menunjukkan bahwa model berhasil mendeteksi semua sampel positif yang benar. *F*1-*score*, yang merupakan rata-rata presisi dan *recall*, menghasilkan nilai sedang, sebesar 49,44%, yang mencerminkan keseimbangan antara presisi dan *recall*. Selain itu, Gambar 1(b) menunjukkan bahwa model tersebut memprediksi 1.919.876 (80,32%) kejadian sebagai TN, 154.435 (13,22%) kejadian sebagai TP, dan tidak ada kejadian



Gambar 1. Perbandingan *confusion matrix*, (a) IF, (b) RBM.

TABEL IV
PERBANDINGAN MENGGUNAKAN METODE YANG ADA

Referensi	Model	Akurasi (%)	Presisi (%)	*Recall* (%)	*F*1-*Score* (%)
[24]	IF (0)	99,62	1,00	1,00	1,00
	IF (1)		0,28	0,29	0,28
[8]	*Rule base* (PaySim)	99,00	99,00	98,00	98,00
	Rule base (BankSim)	99,00	99,00	98,00	98,00
Makalah ini	RBM	87,00	33,00	100,00	49,00
	IF	99,00	98,00	100,00	0,00
	RBM + IF	99,98	100,00	99,00	99,00

yang diprediksi sebagai FN. Namun, terdapat 315.866 (6,46%) kejadian yang diprediksi sebagai FP.

Model ini menunjukkan kecenderungan untuk selalu memprediksi kelas positif dan gagal mendeteksi kelas negatif. Hal ini menunjukkan adanya ketidakseimbangan atau masalah dalam klasifikasi negatif, yang dapat menyebabkan terjadinya galat, terutama jika data kelas negatif digunakan untuk mengidentifikasi pada aplikasi nyata.

D. ANALISIS PERBANDINGAN DENGAN MOTEDE YANG SUDAH ADA

Tabel IV menyajikan hasil evaluasi kinerja dari tiga model klasifikasi yang berbeda, yaitu RBM, pembelajaran mesin, dan kombinasi keduanya (RBM + pembelajaran mesin). Tabel tersebut menunjukkan metrik evaluasi kinerja, termasuk akurasi, presisi, *recall*, dan *F*1-*score*. Model RBM mencapai akurasi sebesar 87% dan presisi sebesar 33%, yang menunjukkan kemampuan model untuk mengidentifikasi secara akurat contoh positif dari semua contoh positif yang diprediksi. Meskipun mencapai *recall* sebesar 100%, *F*1-*score* hanya mencapai 49%, yang menunjukkan ketidakseimbangan antara presisi dan *recall*. Sebaliknya, model pembelajaran mesin menunjukkan akurasi dan presisi yang sangat tinggi. Meskipun demikian, nilai *F*1-*score* hanya menunjukkan 0,0% karena mencapai *recall* 100%, yang menunjukkan kegagalannya dalam mengklasifikasikan contoh negatif. Tabel IV menunjukkan perbandingan hasil kinerja model deteksi transaksi mencurigakan yang diusulkan dalam penelitian ini dengan metode sebelumnya yang digunakan dalam penelitian terkait. Perbandingan ini mencakup beberapa metrik evaluasi utama, yaitu akurasi, presisi, *recall*, dan *F*1-*score*, yang merupakan indikator umum dalam mengukur efektivitas dan akurasi model deteksi. Beberapa metode seperti model IF [24] dan RBM [8] dengan *dataset* PaySim dan BankSim disajikan sebagai acuan untuk melihat perbandingan kinerjanya. Pada penelitian sebelumnya, IF mencatat total 71 galat dengan akurasi 99,72%, sedangkan faktor *outlier* lokal mencatat total 107 galat dengan akurasi 99,62% [24]. Sementara itu, penelitian ini menguji kinerja model IF dan RBM, baik secara sendiri-sendiri maupun gabungan (RBM + IF). Berdasarkan tabel hasil, gabungan RBM + IF menunjukkan kinerja yang sebanding atau bahkan lebih baik dalam beberapa aspek dibanding metode sebelumnya, terutama dari segi akurasi (99,98%) dan presisi (100%), sehingga memperkuat potensi model ini dalam mendeteksi transaksi mencurigakan secara lebih efektif.

V. KESIMPULAN

Untuk mendeteksi transaksi mencurigakan di sektor perbankan, khususnya yang dilakukan melalui kanal daring seperti ATM, *mobile banking*, dan *internet banking*, kombinasi dua model, RBM + IF, terbukti menghasilkan tingkat akurasi yang tinggi. Hal ini dapat menjadi pertimbangan bagi bank untuk melakukan deteksi kecurangan secara cepat dan akurat. Evaluasi pada penelitian ini menunjukkan bahwa kombinasi RBM dan IF menghasilkan kinerja terbaik dengan nilai akurasi, presisi, *recall*, dan *F*1-*score* yang tinggi. RBM mencapai *recall* sempurna, tetapi presisi rendah. Sementara itu, IF mencapai presisi tinggi, tetapi *F*1-*score* rendah karena *recall*-nya buruk. Kombinasi kedua model ini mengatasi kelemahan masing-masing model dan menghasilkan kinerja yang seimbang dengan kinerja yang sangat baik pada semua metrik evaluasi.

Pada implementasi RBM, disarankan untuk menambahkan skenario baru, yaitu penipuan internal yang dilakukan oleh personel bank. IF dapat merekomendasikan aturan baru berdasarkan pembelajaran dari data dan tren penipuan saat ini. Selain itu, berdasarkan hasil RBM yang ada, RBM dapat digunakan untuk memberikan rekomendasi perlunya analisis terhadap transaksi, sebagai penipuan atau normal. Pendekatan ini diharapkan dapat meningkatkan akurasi dan efektivitas sistem deteksi penipuan dalam mengidentifikasi transaksi yang mencurigakan dan mengurangi dampak aktivitas kejahatan keuangan di masa mendatang.

KONFLIK KEPENTINGAN

Penulis menyatakan tidak ada konflik kepentingan.

REFERENSI

[1] B.H. Reddy dan N.T. Rao, "Fraud Detection in Financial Transactions", *Int. J. Eng. Res. Sci. Technol.*, vol. 20, no. 4, hal. 92-98, Nov. 2024.

[2] "Penerapan Strategi Anti Fraud bagi Bank Umum," Peraturan Otoritas Jasa Keuangan, No. 39/POJK.03/2019, 2019.

[3] "Penyedia Jasa Pembayaran," Peraturan Bank Indonesia, No. 23/6/PBI/2021, 2021.

[4] A. Olushola dan J. Mart, "Fraud detection using machine learning," unpublished.

[5] E.R. Kismawadi, U.D.A. Muddatstsir, dan A. Hamid, *Fraud pada Lembaga Keuangan dan Non Keuangan*. Depok, Indonesia: PT. RajaGrafindo Persada, 2020.

[6] R. Abdulahi dan N. Mansor, "Fraud triangle theory and fraud diamond theory. Understanding the convergent and divergent for future research," *Int. J. Acad. Res. Account. Finance Manag. Sci.*, vol. 5, no. 4, hal. 54–64, Des. 2015, doi: 10.6007/ijarafms/v5-i4/1823.

[7] ACFE Indonesia Chapter, "Survei Fraud Indonesia 2019," 2020. [Online]. Tersedia: https://acfe-indonesia.or.id/wp-content/uploads/2021/02/SURVEI-FRAUD-INDONESIA-2019.pdf

[8] S. Islam, M.M. Haque, dan A.N.M.R. Karim, "A rule-based machine learning model for financial fraud detection," *Int. J. Electr. Comput. Eng. (IJECE)*, vol. 14, no. 1, hal. 759–771, Feb. 2024, doi: 10.11591/ijece.v14i1.pp759-771.

[9] M. Baumann, "Improving a rule-based fraud detection system with classification based on association rule mining," dalam *Proc. Ges. Inform.*, 2021, hal. 1121-1134, doi: 10.18420/informatik2021-091.

[10] S. Adewale dan A.B. Madu, "Credit card fraud detection using machine learning,", vol. 9, no. 4, hal. 11, 2020, doi: 10.13140/RG.2.2.36291.53287.

[11] I. Nwade dkk., "Development of credit cards fraud detection model," *LAUTECH J. Eng. Technol.*, vol. 17, no. 2, hal. 1–8, Jul. 2023.

[12] M.G. Saragih dkk., "Machine learning methods for analysis fraud credit card transaction," *Int. J. Eng. Adv. Technol. (IJEAT)*, vol. 8, no. 6S, hal. 870–874, Agu. 2019, doi: 10.35940/ijeat.F1164.0886S19.

[13] A. Bănărescu, "Detecting and preventing fraud with data analytics," *Procedia Econ. Finance*, vol. 32, hal. 1827–1836, 2015, doi: 10.1016/s2212-5671(15)01485-9.

[14] M. Pełka dan A. Dudek, "Isolation forests for symbolic data as a tool for outlier mining," *Econom., Ekonom., Adv. Appl. Data Anal.*, vol. 28, no. 1, hal. 1–10, Jan. 2024, doi: 10.15611/eada.2024.1.01.

[15] M.K.M. Almansoori dan M. Telek, "Anomaly detection using combination of autoencoder and isolation forest," dalam *1st Workshop Intell. Infocommunication Netw. Syst. Serv. (WI2NS2)*, 2023, hal. 25–30, doi: 10.3311/wins2023-005.

[16] A. Nursanti dan I. Trinugroho, "The effect of financial literacy on the ability to detect investment fraud," *Int. J. Soc. Sci. Res. Rev.*, vol. 6, no. 12, hal. 323–337, Des. 2023, doi: 10.47814/ijssrr.v6i12.1840.

[17] K.F. Andriani, K. Budiartha, M.M.R. Sari, dan A.A.G.P. Widanaputra, "Fraud pentagon elements in detecting fraudulent financial statement," *Linguist. Cult. Rev.*, vol. 6, hal. 686–710, Jan. 2022, doi: 10.21744/lingcure.v6ns1.2145.

[18] M. Sirigineedi dkk., "Fake credit transaction detection using machine learning," *Int. J. Res. Sci. Eng.*, vol. 4, no. 3, hal. 1–9, Apr./Mei 2024, doi: 10.55529/ijrise.43.1.9.

[19] E. Pan, "Machine learning in financial transaction fraud detection and prevention," *Trans. Econ. Bus. Manag. Res.*, vol. 5, hal. 243-249, Mar. 2024, doi: 10.62051/16r3aa10.

[20] H. Kamel dan M.Z. Abdullah, "Distributed denial of service attacks detection for software defined networks based on evolutionary decision tree model," *Bull. Electr. Eng. Inform.*, vol. 11, no. 4, hal. 2322–2330, Agu. 2022, doi: 10.11591/eei.v11i4.3835.

[21] N.S. Arunraj dkk., "Comparison of supervised, semi-supervised and unsupervised learning methods in network intrusion detection system (NIDS) application," *AKWI*, no. 6, hal. 10–19, Des. 2017, doi: 10.26034/lu.akwi.2017.3183.

[22] G.M. Rao dan D. Ramesh, "Ranger random forest-based efficient ensemble learning approach for detecting malicious URLs," dalam *Proc. Int. Conf. Recent Trends Mach. Learn. IoT Smart Cities Appl.*, V.K. Gunjan dan J.M. Zurada, Eds., 2020, hal. 599-608, doi: 10.1007/978-981-15-7234-0_56.

[23] M.I. Akazue dkk., "UNMASKING FRAUDSTERS: Ensemble features selection to enhance random forest fraud detection," *J. Comput. Theor. Appl.*, vol. 1, no. 2, hal. 201–211, Des. 2023, doi: 10.33633/jcta.v1i2.9462.

[24] V. Vijayakumar, N.S. Divya, P. Sarojini, dan K. Sonika, "Isolation forest and local outlier factor for credit card fraud detection system," *Int. J. Eng. Adv. Technol. (IJEAT)*, vol. 9, no. 4, hal. 261–265, Apr. 2020, doi: 10.35940/ijeat.D6815.049420.

[25] M.L.V. Nalupa, J.R.D. Fernandez, W.J.C. Dacay, dan M.M. Bergado, "Fraud detection using isolation forest for RFID-based attendance monitoring system," *Sci. Int.*, vol. 6, no. 34, hal. 511-517, Des. 2022.

[26] A. Zulfikar, F.A. Rahmani, dan N. Azizah, "Deteksi anomali menggunakan isolation forest belanja barang persediaan konsumsi pada satuan kerja Kepolisian Republik Indonesia," *J. Manaj. Perbendaharaan*, vol. 4, no. 1, hal. 1–15, Jun. 2023, doi: 10.33105/jmp.v4i1.435.

[27] H. John dan S. Naaz, "Credit card fraud detection using local outlier factor and isolation forest," *Int. J. Comput. Sci. Eng.*, vol. 7, no. 4, hal. 1060–1064, Apr. 2019, doi: 10.26438/ijcse/v7i4.10601064.