DIPONEGORO JOURNAL OF ACCOUNTING *Volume 13, Nomor 3, Tahun 2024, Halaman 1-15*
http://ejournal-s1.undip.ac.id/index.php/accounting ***ISSN (Online): 2337-3806***

PENERAPAN *MACHINE LEARNING* DAN *DEEP LEARNING* PADA PENINGKATAN DETEKSI *CREDIT CARD FRAUD - A SYSTEMATIC LITERATURE REVIEW*

Berliana Via Tarissa, Totok Dewayanto[1]

Departemen Akuntansi Fakultas Ekonomika dan Bisnis Universitas Diponegoro
Jl.Prof. Soedharto SH Tembalang, Semarang 50239, Phone: +6282135240978

ABSTRACT

This research aims to explore the application of machine learning and deep learning in enhancing credit card fraud detection and identifying gaps in knowledge that could serve as a foundation for future research.

The study utilized the systematic literature review (SLR) method to analyze various articles published in Scopus-indexed journals between 2020 and 2024. Article selection followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, resulting in the inclusion of twenty top-tier articles based on predefined keywords.

The findings indicate that machine learning and deep learning significantly improve the accuracy and efficiency of fraud detection by effectively identifying complex fraud patterns that are challenging to detect using traditional methods, thereby reducing false alarms. Several algorithms such as Random Forest, XGBoost, Convolutional Neural Network (CNN), and Long Short-Term Memory (LSTM) demonstrated high performance in classifying transactions as legitimate or fraudulent. The integration of these algorithms also has the potential to enhance overall system performance. The implementation of machine learning and deep learning not only strengthens the security of current fraud detection systems but also prepares financial institutions to tackle future challenges. Further adaptation to increasingly complex fraud patterns is crucial for enhancing financial transaction security in the digital era. Therefore, the development of more innovative and adaptive algorithm combinations is necessary to meet the growing security demands in the modern financial world.

Keywords: machine learning, deep learning, credit card fraud detection, financial industry, SLR

PENDAHULUAN

Perkembangan teknologi telah mengubah cara transaksi keuangan, dengan transaksi online dan pengggunan kartu kredit menjadi dominan. Namun, penipu sering menggunakan informasi kartu kredit, seperti nomor kartu dan kode keamanan untuk melakukan transaksi penipuan secara online(Pandey et al., 2018). Adanya pandemi covid-19 mendorong lonjakan penggunaan kartu kredit dalam transaksi daring. Hal tersebut membuka peluang bagi pelaku kejahatan untuk memanfaatkan situasi. Dampaknya tidak hanya terbatas pada kerugian finansial, tetapi potensi pencurian identitas yang serius. Dalam konteks ini, penting bagi masyarakat untuk meningkatkan kewaspadaan dan kebijaksanaan dalam melakukan transaksi online, serta untuk selalu memverifikasi keamanan dan keaslian situs e-commerce sebelum memberikan informasi sensitif seperti data kartu kredit.

Teknologi telah menyederhanakan proses transaksi secara global, perkembangan tersebut juga membawa risiko yang signifikan terhadap keamanan data pribadi dan finansial pengguna. Chaudhary et al., (2012) menyoroti bahwa penipuan kartu kredit saat ini telah menjadi masalah yang semakin meningkat di industri kartu kredit. Berdasarkan data statistik yang dipublikasikan SPIP pada bulan Juni tahun 2022, terlihat adanya tren kenaikan signifikan dalam sirkulasi kartu kredit. Ningsih et al., (2022) menggambarkan fenomena ini menjadi salah satu faktor yang membuat kartu kredit menjadi target utama tindak kejahatan dengan memanfaatkan kebocoran data pribadi pemilik kartu kredit.

Meningkatkan akurasi deteksi dan kemampuan komputasi mengingat kumpulan data perdagangan yang berkembang pesat adalah masalah utama yang dihadapi oleh sebagian besar *credit*

[1] *Corresponding author*

card fraud(Pandey et al., 2018). Perkembangan big data telah membawa dampak signifikan dalam deteksi fraud, terutama dalam konteks keuangan(Syahputra & Afnan, 2020). Namun, Banyak peneliti telah beralih ke cabang kecerdasan buatan ini untuk menemukan jawaban atas berbagai masalah. Karena penipuan kartu kredit tidak dapat ditangani dengan baik oleh manusia, maka *machine learning* harus digunakan untuk menyelesaikan masalah tersebut(Paruchuri, 2017).

Pendekatan *machine learning* diperlukan untuk menjamin penipuan transaksi kartu kredit. Algoritma ML menawarkan potensi deteksi penipuan yang lebih cepat dan akurat. Namun, tantangannya terletak pada pemilihan algoritma yang paling efektif, terus memperbarui model deteksi penipuan, dan menyeimbangkan deteksi yang akurat untuk meminimalkan positif palsu(Paruchuri, 2017). Hal tersebut juga ditekankan Moh. Badris Sholeh Rahmatullah et al., (2022) bahwa tantangan dan pendekatan dalam mendeteksi penipuan kartu kredit yaitu teknik penipuan yang berkembang membutuhkan pembaruan dan peningkatan konstan pada sistem deteksi penipuan, keamanan yang kuat, kumpulan data tidak seimbang. Sehingga penggunaan *deep learning* diperlukan bagaimana akurasi dan presisi dalam deteksi *credit card fraud*.

Penggunaan teknologi memperlihatkan keefektifannya dalam mendeteksi penipuan termasuk kartu kredit. *Machine learning* mengenali pola data yang kompleks, sementara *deep learning* menggunakan jaringan neural untuk memproses data yang lebih kompleks. Integrasi ML dan DL meningkatkan efektivitas deteksi penipuan. (Cherif et al., 2023) menyebutkan bahwa pendekatan berbasis ML dan DL dapat meningkatkan efisiensi dan keakuratan deteksi penipuan kartu kredit.

Dengan demikian, berikut adalah pertanyaan penelitian pada penelitian ini:

RQ1: Bagaimana penerapan *machine learning* dan *deep learning* yang dieksplor dalam meningkatkan kinerja deteksi penipuan kartu kredit?

RQ2 : Apa dampak positif dari penggunaan *machine learning* dan *deep learning* dalam deteksi penipuan kartu kredit?

Penelitian ini bertujuan untuk Menyusun sebuah tinjauan literatur yang sistematis berkaitan dengan penerapan *machine learning* dan *deep learning* dalam upaya peningkatan deteksi penipuan kartu kredit dengan menggali beragam hasil penelitian yang relevan pada penelitian empiris dan melakukan sintesis pada temuan yang didapat.

TINJAUAN PUSTAKA DAN KERANGKA PEMIKIRAN TEORITIS

Bagian ini menjelaskan teori dan konsep serta kerangka pemikiran yang digunakan dalam penelitian.

Teori Difusi Inovasi

Teori difusi inovasi ini berfokus pada pengembangan tentang bagaimana, mengapa, dan dengan seberapa cepat gagaran dan teknologi inovatif menyebar dalam suatu sistem sosial (Ahmad Wani & Wajid Ali, 2015). Dalam konseptualisasi Everett Rogers (2003), Menurut Everett Rogers (2003), difusi adalah proses penyebaran inovasi melalui jalur tertentu dalam kelompok sosial selama waktu tertentu, menjadikannya bentuk komunikasi khusus untuk mencapai pemahaman bersama. Inovasi adalah konsep, tindakan, atau objek baru bagi individu atau pengadopsi, dengan fokus utama pada inovasi teknologi(García-Avilés, 2020).

Theory Diffusion of Innovation oleh Rogers mengidentifikasi lima atribut inovasi yang mempengaruhi penerapannya, termasuk keunggulan relatif, kesesuaian, kompleksitas, kemampuan untuk dicoba, dan kemampuan observasi. (García-Avilés, 2020). *Theory diffusion of innovation* memainkan peran penting dalam deteksi penipuan kartu kredit dengan memfasilitasi pemahaman evolusi sistem dan pembangunan solusi, termasuk teknologi deteksi penipuan. Dengan bantuan teori difusi inovasi, dapat dipahami bagaimana sistem-sistem beradaptasi terhadap perubahan lingkungan dan kebutuhan pengguna, terutama dalam konteks keamanan transaksi finansial.

Big Data

Big data didefinisikan sebagai sekumpulan data yang memiliki volume, kompleksitas, dan variasi yang besar sehingga sulit untuk dikelola menggunakan metode konvensional.(Herland et al., 2018). Dalam akuntansi modern, *big data* menjadi salah satu konsep penting. Dalam pencegahan dan

deteksi *fraud, big data* memiliki peran signifikan dengan menganalisis pola transaksi pengguna(Balasupramanian et al., 2017;Jha et al., 2020)

Penggunaan *big data* dalam deteksi fraud telah mengubah paradigma keamanan bisnis dengan memanfaatkan kekuatan analisis data yang canggih dengan melalui beragam metode.. Dalam upaya mencegah penipuan(Razaque et al., 2023) menyoroti berbagai teknik *big data*, seperti analisis regresi, korelasi, dan analisis statistik deskriptif, digunakan untuk mengidentifikasi pola perilaku penipuan.

Machine Learning

Machine learning adalah cabang dari kecerdasan buatan yang berfokus pada pengembangan algoritma dan memungkinkan model dapat belajar dari data dan membuat prediksi tanpa harus diprogram secara eksplisit(Ali et al., 2022). Dalam konteks deteksi *fraud, machine learning* memiliki peran yang sangat penting, khususnya pada *credit card fraud.* Bank menggunakan berbagai metode *machine learning* untuk memprediksi *fraud*, dengan memanfaatkan data historis dan fitur-fitur baru guna meningkatkan ketepatan prediksi(V S S & Deepthi Kavila, 2018). *Machine learning* dapat mengotomasikan proses mendeteksi penipuan dengan menganalisis transaksi secara *real-time.* Dengan merancang dan menerapkan algoritma atau model yang efisien dapat menangani volume besar data tepat waktu dan akurat pada deteksi ataupun pencegahan kegiatan penipuan(Gwale & Sharma, 2023)

Deep Learning

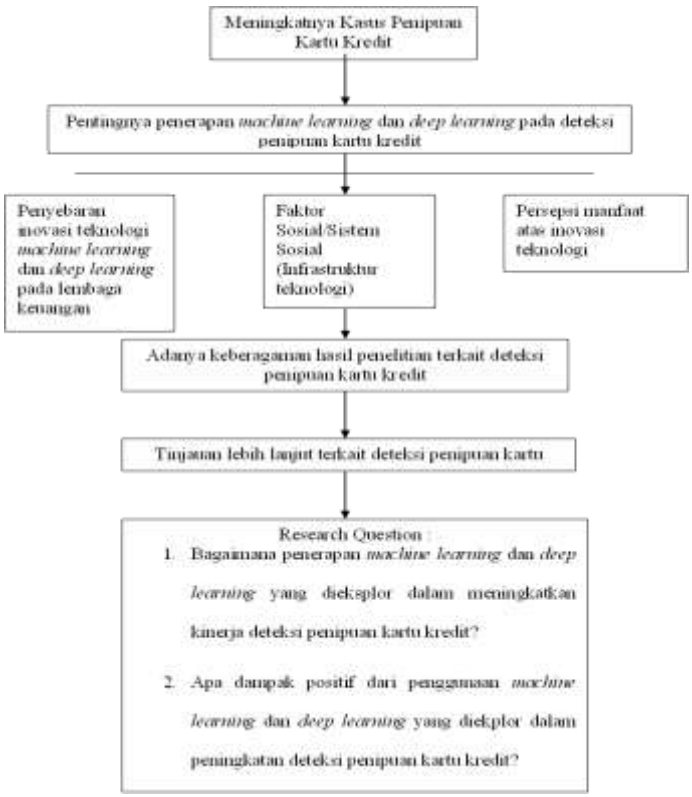
Deep Learning adalah sub-bidang *machine learning* yang berfokus pada pelatihan jaringan saraf buatan dengan beberapa lapisan untuk belajar dan membuat prediksi dari data yang kompleks. Algoritma *deep learning* menggunakan proses yang disebut *backpropagasi* untuk menyesuaikan bobot dan bias neuron, mengoptimalkan kinerja jaringan dari waktu ke waktu. Teknik ini memungkinkan model *deep learning* untuk secara otomatis mempelajari dan mengekstrak fitur yang relevan dari data, tanpa perlu rekayasa fitur manual(Ingole et al., 2023)

Deteksi kecurangan dalam transaksi keuangan adalah salah satu area di mana *deep learning* dapat memiliki pengaruh yang signifikan(Roy et al., 2018). Alasan *deep learning* menjadi popular karena kemajuan yang signifikan dalam kemampuan pemrosesan chip, sehingga mempercepat proses pelatihan dan pengujian, dan biaya komputasi perangkat keras yang semakin rendah telah mempermudah aksesibilitas teknologi *deep learning*(Shinde & Shah, 2018).

Kerangka Pemikiran

Kerangka pemikiran teoritis yang digunakan dalam penelitian ini adalah sebagai berikut

Gambar 1
Kerangka Pemikiran Teoritis



METODE PENELITIAN

Bagian ini menjelaskan perumusan pertanyaan penelitian, strategi pencarian literatur, kriteria literatur, dan seleksi literatur.

Perumusan Masalah Penelitian

Dalam penelitian ini, untuk merumuskan masalah penelitian akan menggunakan kerangka kerja *Population, Intervention, Comparison,* idan *Outcome* (PICO) yang digunakan untuk membantu peneliti Menyusun pertanyaan penelitian sehingga memudahkan dalam pencarian literatur yang relevan dan akurat.

Tabel 1
***Framework* PICO**

PICO Tool	
Population	Lembaga keuangan
Intervention	*Machine learning* dan *deep learning*
Comparison	-
Outcome	Deteksi penipuan kartu kredit

Sumber:Analisis Artikel.2024

Berdasarkan kerangka PICO yang dirumuskan tersebut, kata kunci yang digunakan adalah *machine learning*, *deep learning*; *credit card fraud detection*; dan *financial institutions*. Kata kunci tersebut merupakan kata kunci dasar yang akan dikembangkan saat melakukan pencarian literatur.

Pencarian Literatur

Sumber data yang digunakan dalam penelitian ini adalah data sekunder yang terdiri dari hasil-hasil penelitian yang telah dipublikasikan dalam secara online. Untuk melakukan pengumpulan data, pencarian dilakukan melalui basis data ilmiah yaitu Scopus dalam bentuk artikel jurnal. Proses pencarian artikel dilakukan dengan menyusun kombinasi kata kunci yang relevan yaitu (AND,OR) berdasarkan analisis PICO.

Kata kunci yang digunakan oleh peneliti adalah *(("financial institution" OR "Bank") AND ("deep learning" OR "machine learning") AND ("fraud" OR "fraudulant" OR "credit card fraud" OR "card fraud" OR "card skimming" OR "carding" OR "payment card fraud"))*

Kriteria Literatur

Kriteria literatur terdiri dari kriteria inklusi dan eksklusi, yang disesuaikan berdasarkan kerangka kerja PICO yang telah dibuat sebelumnya. Berikut adalah penjelasan mengenai dua kriteria tersebut:

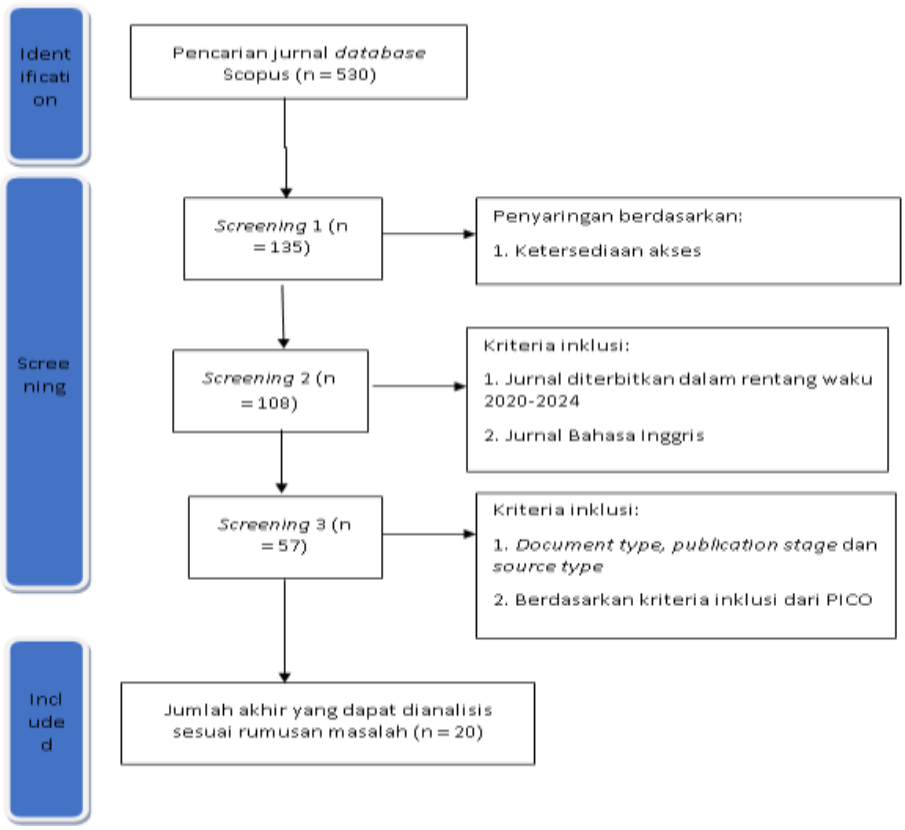
Tabel 2
Kriteria Eksklusi dan Inklusi

Kriteria	Inklusi	Eksklusi
Bahasa	Inggris	Tidak dalam bahasa Inggris
Keterbukaan akses	Artikel penelitian yang dapat diakses secara *full text*	Artikel penelitian yang berbayar atau tidak dapat diakses secara *full text*
Jenis Dokumen	*Original research*	*Article review*
Jangka Waktu	Maksimal 4 tahun terakhir (2020-2024)	Penerbitan artikel kurang dari tahun 2020
Tema Isi Jurnal	Membahas mengenai penerapan *machine learning dan deep learning* pada penipuan kartu kredit	Artikel yang setelah dianalisis mendalam tidak sesuai dengan permasalahan penelitian

Seleksi Literatur

Data dikumpulkan melalui database Scopus dan dianalisis menggunakan kerangka kerja PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta Analyses*) yang terdiri dari 3 tahapan sebagai berikut

Gambar 2
PRISMA *Flow Diagram*



Sumber:Analisis Artikel,2024

HASIL PENELITIAN DAN PEMBAHASAN

Bagian ini berisi pembahasan temuan hasil penelitian dan sintesis temuan hasil penelitian.

Temuan Hasil Penelitian

Temuan hasil dibagi menjadi 2 yaitu penerapan *machine learning* pada peningkatan deteksi penipuan kartu kredit dan penerapan *deep learning* pada peningkatan deteksi penipuan kartu kredit.

Penerapan *Machine Learning* pada Peningkatan Deteksi Penipuan Kartu Kredit

Tabel 3
Penerapan *Machine Learning* pada Peningkatan Deteksi Penipuan Kartu Kredit

No	Judul Artikel	Peneliti	Temuan
1.	*Credit card fraud detection using a new hybrid machine learning architecture*	Esraa Faisal Malik, Khai Wah Khaw, Bahari Belaton, Wai Peng Wong, XingYing Chew (2022)	Studi ini menyoroti efektivitas model hibrida Adaboost+LGM dalam mendeteksi kegiatan penipuan kartu kredit. Model hibrida terbaik, Adaboost LGBM, menegaskan keefektifan penerapan *machine learning* dalam mendeteksi penipuan kartu kredit dilihat pada hasil

2	*A novel method for detecting credit card fraud problem*	Hai Chao DU, Li Lv, Hongliang Wang, An Guo (2024)(H. C. Du et al., 2024)	Studi ini mengusulkan pendekatan oversampling dua fase. Pendekatan ini menggabungkan autoencoder, XGBoost, SMOTE, dan GAN untuk mengatasi ketidakseimbangan kelas dengan menghasilkan distribusi data yang realistis. Melalui perbandingan dengan algoritma lain, studi menunjukkan peningkatan signifikan dalam akurasi deteksi penipuan. Keseluruhan, artikel ini membahas pendekatan inovatif untuk meningkatkan efektivitas deteksi penipuan kartu kredit.
3	*A Smote based Oversampling Data-Point approach to solving the credit card data imbalance problem in financial fraud detection*	Nhlakanipho Mqadi, Nalindren Naicker, Timothy Adeliyi (2021)	Mengkaji penggunaan teknik Oversampling SMOTe untuk meningkatkan deteksi penipuan kartu kredit dalam data yang tidak seimbang. Penelitian ini menguji efektivitas beberapa algoritma pembelajaran mesin dalam mengidentifikasi transaksi penipuan setelah menerapkan teknik oversampling pada dataset. Hasilnya menunjukkan peningkatan dalam deteksi transaksi penipuan, yang diukur melalui beberapa metrik evaluasi.
4	*Utilizing GANs for Credit Card Fraud Detection : A comparison of supervised learning algorithm*	Bandar Alshawi (2023)	Penelitian ini menemukan bahwa penggunaan Generative Adversarial Networks (GAN) efektif dalam mendeteksi penipuan kartu kredit, terutama pada dataset yang kecil dan tidak seimbang. Enam algoritma pembelajaran mesin dievaluasi, dan semuanya menunjukkan hasil yang mengesankan. XGBoost mencatat kinerja terbaik dengan mencapai tingkat akurasi tertinggi
5	*Machine learning model for credit card fraud detection-a comparative analysis*	Pratyush Sharma, Souradeep Banerjee, Devyanshi Tiwari, Jagdish Chandra Patni (2021)	Penelitian ini bertujuan untuk mengevaluasi kinerja berbagai model pembelajaran mesin dalam deteksi penipuan kartu kredit. Dengan menggunakan dataset dari Kaggle yang melibatkan ratusan ribu titik data dan 31 kolom fitur, penelitian ini membandingkan beberapa algoritma machine learning.
6	*Ensemble learning with supervised machine learning models to predict credit card fraud transaction*	Mohammed Rashad Baker, Zuhair Norii Mahmood, Ehab Hashim Shaker (2022)	Penelitian ini menunjukkan bahwa teknik pembelajaran ensemble, khususnya metode ensemble pemungutan suara yang menggunakan PCA, sangat efektif dalam mendeteksi transaksi penipuan kartu kredit. Teknik ini berhasil mengungguli metode pembelajaran mesin lainnya dan kinerja deteksi penipuan.Temuan ini menegaskan potensi besar dari model pembelajaran ansambel, terutama ketika dikombinasikan dengan teknik pengurangan dimensi, dalam memprediksi transaksi penipuan dengan lebih akurat dan efisien.

7	*A soft voting ensemble learning approach for credit card fraud detection*	Mimusa Azim Mim, Nazia Majadi, Peal Mazumder (2024)	Menguji penerapan pendekatan pembelajaran ansambel pemungutan suara lunak untuk mendeteksi penipuan kartu kredit pada data yang tidak seimbang. Hasil eksperimen menunjukkan bahwa pendekatan tersebut menghasilkan kinerja yang superior. Pendekatan ansambel menunjukkan keunggulan yang signifikan, menekankan pentingnya metode ansambel dalam menangani ketidakseimbangan data dalam tugas klasifikasi yang serupa.
8	*Example-dependent cost-sensitive credit card fraud detection using SMOTE and Bayes minimum risk*	Doaa Almhaithawi, Assef Jafar, Mohamad Aljnidi (2020)	Temuan utama dari artikel menyoroti efektivitas berbagai algoritma dan teknik penyeimbangan data dalam deteksi penipuan kartu kredit. Hasil penelitian menunjukkan bahwa XGBoost (XG) menunjukkan kinerja yang menjanjikan dalam mendeteksi kasus penipuan, terutama bila dikombinasikan dengan teknik seperti SMOTE dan risiko minimum Bayes (BMR).
9	*Federated learning model for credit card fraud detection with data balancing techniques*	Mustafa Abdul Salam, Khaled M.Fouad, Doaa L. Elbably, Salah M. Elsayed (2024)	Studi ini menemukan bahwa teknik resampling hibrida meningkatkan kinerja model deteksi penipuan kartu kredit, dengan Random Forest menunjukkan akurasi terbaik. *Federated learning* dengan PyTorch memberikan akurasi lebih tinggi, meskipun dengan waktu komputasi yang lebih lama. Pendekatan ini memungkinkan kolaborasi antar bank tanpa mengorbankan privasi data.
10	*Cybersecurity enhancement to detect credit card fraud in helath care using new machine learning strategies*	E Jayanthi, T Ramesh, Reena S Kharat, M R M Veeramanickam, N Bharathiraja, R Venkatesan, Raja Marappan (2023)	Studi ini menemukan bahwa penggunaan strategi pengklasifikasi baru, seperti pohon keputusan berbasis cluster dan klasifikasi, regresi logistik, dan hutan acak, dapat meningkatkan deteksi penipuan dalam transaksi kartu kredit di sektor perawatan kesehatan. Analisis hasil menunjukkan bahwa strategi tersebut berhasil mencapai akurasi, presisi, sensitivitas, dan spesifisitas yang tinggi, mengungguli metode yang sudah ada. Temuan ini memberikan kontribusi signifikan dalam meningkatkan langkah-langkah keamanan siber dalam mengatasi aktivitas penipuan dalam skala besar, dengan memanfaatkan teknik pembelajaran mesin yang inovatif.
11	*Some insight about applicability of logistic factorisation machine in banking*	Erika Slabber, Tanja Verster, Riaan de Jongh (2023)	Studi menemukan bahwa Mesin Faktorisasi Logistik (LFM) dalam machine learning memiliki kinerja yang kuat dalam berbagai kasus, termasuk memberi rekomendasi, mendeteksi penipuan kartu kredit, dan menilai kredit. Evaluasi model menyoroti pentingnya memilih algoritma yang sesuai untuk setiap masalah yang dihadapi.

12	*Credit card fraud detection using fuzzy rough nearest neighbor and sequential minimal optimization with logistic regression*	Ameer Saleh Hussein, Rihab Salah, Khairy, Shaima Miqdad Mohamed Najeeb, Haider Th Salim Alrikabi (2021)	Penelitian ini menemukan bahwa model ensemble yang menggabungkan berbagai pengklasifikasi, seperti FRNN, SMO, dan LR, berhasil mencapai tingkat deteksi yang baik dalam mendeteksi penipuan kartu kredit. Ini menyoroti pentingnya pendekatan yang terpadu dalam memerangi kejahatan keuangan dan melindungi konsumen serta lembaga keuangan dari kerugian finansial yang signifikan.
13	*Performance evaluation of machine learning methods for credit card fraud detection using SMOTE and AdaBoost*	Emmanuel Ileberi, Yanxia Sun, Zenghui Wang (2021)	Studi ini menemukan bahwa penggunaan teknologi pembelajaran mesin dengan SMOTE dan ADABoost dapat meningkatkan deteksi penipuan kartu kredit, membantu melindungi transaksi keuangan dan mengurangi risiko kerugian bagi institusi keuangan dan konsumen.
14	*Detecting fraud transaction using ripper algorithm combines with ensemble learning model*	Vo Hoang Khang, Cao Tung Anh, Nguyen Dinh Thuan (2023)	Penelitian menemukan bahwa kombinasi dengan metode Ensemble Learning, terutama Gradient Boosting, mampu mendeteksi penipuan kartu kredit dengan keandalan yang tinggi. Hal ini menyoroti pentingnya pengembangan solusi deteksi penipuan yang efektif. Meskipun menggunakan beberapa model dapat meningkatkan kinerja, ini juga memerlukan lebih banyak sumber daya. Namun, manfaatnya diyakini lebih besar daripada tantangan yang dihadapi.
15	*Class balancing framework for credit card fraud detection based on clustering and similarity-based selection(SBS)*	Hadeel Ahmad, Bassam Kasasbeh, Balqeeh Aldabaybah, Enas Rawashdeh (2022)	Penelitian ini menemukan bahwa teknik Seleksi Berbasis Kemiripan (SBS) mengungguli metode lain dalam deteksi penipuan kartu kredit, dengan peningkatan signifikan dalam akurasi, sensitivitas, dan spesifisitas. Algoritma Artificial Neural Network (ANN) terbukti paling efisien dalam menghindari alarm palsu, menunjukkan keunggulan dalam mengatasi kelas yang tidak seimbang.

Penelitian diatas memberikan kesimpulan bahwa berbagai efektivitas teknik ML terbukti efektif dalam mendeteksi penipuan kartu kredit dengan teknik SMOTE membantu mengatasi ketidakseimbangan data dan meningkatkan akurasi model. Selain itu ditekankannya untuk memilih algoritma yang sesuai setiap tugas atau dataset untuk meningkatkan kinerja prediksi dan pemisahan data. Dalam mengevaluasi deteksi penipuan perlu teknik pengurangan dimensi dan evaluasi yang tepat dengan parameter presisi, ingatan, AUROC, Tingkat negative palsu dan skor F1. Selain itu, pendekatan teknik baru dan integrasi baru dapat meningkatkan keamanan siber dan mitigasi risiko. Pendekatan ini tidak hanya di industri keuangan tetapi juga sektor lain seperti perawatan Kesehatan, menunjukkan peningkatan keamanan dan efektivitas deteksi penipuan.

Penerapan *Deep Learning Learning* pada Peningkatan Deteksi Penipuan Kartu Kredit

Tabel 4
Penerapan *Deep Learning* pada Peningkatan Deteksi Penipuan Kartu Kredit

No.	Judul Artikel	Peneliti	Temuan
1.	*Autoencoder and lightGBM for credit card fraud detection problems*	Haichao Du, Li Lv, An Guo Hongliang Wang (2023)	Studi ini menyoroti hasil signifikan dalam deteksi penipuan kartu kredit menggunakan algoritma AED-LGB. Dibandingkan dengan algoritma pembelajaran mesin tradisional, AED-LGB menunjukkan kinerja yang lebih baik dalam akurasi, serta unggul dalam menangani kumpulan data yang tidak seimbang. Integrasi autoencoder dengan LightGBM berhasil meningkatkan pembelajaran representasi fitur dan kinerja klasifikasi, menegaskan efektivitas pendekatan gabungan ini dalam meningkatkan deteksi penipuan kartu kredit
2	*Enhanced credit card fraud detection based on attention mechanism and LSTM deep model*	Ibtissam Benchaji, Samira Douzi, Bouabid El Ouahidi, Jaafar Jafari (2021)	Studi menunjukkan bahwa model LSTM yang ditingkatkan dengan kemampuan fokus pada detail-detail penting, mengungguli model dasar dalam mendeteksi penipuan kartu kredit. Dengan fokus pada pola transaksi yang relevan, model ini berhasil mengidentifikasi transaksi penipuan dengan lebih akurat, memberikan kontribusi penting bagi keamanan layanan keuangan.
3	*CTCN : a novel credit card fraud detection method based on conditional tabular generative adversarial networks and temporal convolutional network*	Xiaoyan Zhao, Shaopeng Guan (2023)	Penelitian menemukan bahwa pendekatan baru, CTCN, yang menggabungkan CTGAN dan TCN, lebih efektif dalam mendeteksi penipuan kartu kredit daripada metode tradisional. Ini terbukti dari hasil eksperimen yang menunjukkan peningkatan signifikan dalam akurasi dan kinerja deteksi.
4	*A systematic review of literature on credit card fraud detection using machine learning and deep learning*	Eyad Abdel Latif Marazqah Btoush, Xujuan Zhou, Raj Gururajan, Ka Ching Chan, Rohan Genrich, Prema Sankaran (2023)	Hasil penelitian menunjukkan bahwa sebagian besar artikel tentang deteksi penipuan kartu kredit lebih cenderung menggunakan teknik supervised learning, dengan 74% artikel menerapkan pendekatan ini. Di samping itu, terdapat peningkatan minat dalam penggunaan teknik deep learning dari tahun 2019 hingga 2021. Hal ini tercermin dari banyaknya jumlah artikel yang menggunakan teknik deep learning.

5	*High-Cardinality categorical attributes and credit card fraud detection*	Emmanuel Mineda Carneiro, Carlon Henrique Quartucci Forster, Linei Fernando Stege Mialaret, Luiz Alberto, Adilson Marques (2022)	Penelitian ini mengembangkan VCCA sebagai pendekatan baru untuk pengurangan domain yang bertujuan untuk mempertahankan kemampuan deteksi penipuan sambil meningkatkan waktu pelatihan model dengan mempertahankan keuntungan dari atribut dengan kardinalitas tinggi

Penelitian diatas memberikan kesimpulan bahwa penggunaan teknologi *deep learning* seperti autoencoder,LSTM, CTGA, dan TCN meningkatkan deteksi penipuan kartu kredit dengan menyesuaikan ambang probabilitas klasifikasi. Penerapan supervised learning juga ditekankan mengembangkan dalam model adaptif untuk memberikan kontribusi signifikan dalam meningkatkan efektivitas sistem deteksi penipuan. Pentingnya evaluasi yang cermat terhadap berbagai algoritma seperti FNN dan teknik clustering tidak hanya meningkatkan kualitas deteksi tetapi juga mengurangin waktu pelatihan. Temuan ini memiliki implikasi signifikan bagi industri keuangan, menawarkan landasan yang kuat untuk pengembangan sistem deteksi penipuan yang lebih efisien dan responsive terhadap ancaman yang semakin kompleks.

Sintesis Temuan Hasil Penelitian

Bagian ini menyajikan sintesis dari 20 artikel temuan yang secara khusu dirancang untuk menjawab pertanyaan penelitian atau *research question* (RQ).

Kekuatan dan Kelemahan *Machine Learning* dan *Deep Learning* pada Deteksi Penipuan Kartu Kredit

Dalam kinerja dan efektivitas dari setiap algoritma perlu memahami kekuatan dan kelemahan masing-masing algoritma dalam menangani dataset penipuan transaksi keuangan untuk membantu memilih metode yang paling tepat untuk implementasi praktis.

Tabel 6
Persentase Penilaian *Machine Learning* dalam Deteksi Penipuan Kartu Kredit

Algoritma	Kekuatan (%)	Kelemahan (%)
Naif Bayes(NB)	89	11
AdaBoost	97	3
XGBoost	98	2
LightBGM(LGBM)	82	18
Random Forest(RF)	98	2
KNN	90	10
SVM	95	5
DT	95	5
LR	96	4
ANN	99	1
LFM	99	1

FRNN	81	19

Sumber:Analiss Artikel,2024

Tabel 7
Persentase Penilaian *Deep Learning* dalam Deteksi Penipuan Kartu Kredit

Algoritma	Kekuatan (%)	Kelemahan (%)
Jaringan saraf *feed forward* (FNN)	85	15
Jaringan saraf konvolusional(CNN)	89	11
Multiplayer Perceptron (MLP)	88	12
Jaringan saraf rekuren(RNN)	90	10
Long-Short Term Memory (LSTM)	92	8
Jaringan saraf konvolusional dalam(DCNN)	88	12
Jaringan saraf dalam(DNN)	94	6
Autoencoder(AE)	82	18
Generative Adversarial Network (GAN)	85	15

Sumber:Analisis Artikel,2024

Integrasi *Machine Learning dan Deep Learning* pada Peningkatan Deteksi Penipuan Kartu Kredit

Dalam kinerja dan efektivitas dari ML dan DL masih memiliki kelemahan dan kelebihan. Sehingga hal tersebut bisa dieksplorasi lebih banyak. Integrasi algoritma adalah salah satu upaya untuk mengatasi hal tersebut. Integrasi *Naïve Bayes* (NB) dan *Deep Neural Network* (DNN) menjanjikan sebuah pendekatan yang komprehensif dimana NB memberikan kerangka awal yang cepat dan sederhana untuk mengenali pola dasar dari data transaksi. Sementara itu, DNN dapat digunakan untuk menangkap pola yang lebih abstrak, terutama dalam menangani ketergantungan antar fitur yang lebih rumit. Integrasi ini memungkinkan penggunaan output untuk DNN. Kombinasi keduanya tidak hanya meningkatkan keandalan deteksi, tetapi juga memberikan dasar interpretative yang kuat untuk Keputusan yang lebih tepat waktu dan efektif dalam mengamankan transaksi keuangan.

Dampak Positif Penerapan *Machine Learning* dan *Deep Learning* pada Peningkatan Deteksi Penipuan Kartu Kredit

Penerapan teknologi pembelajaran mesin (ML) dan pembelajaran mendalam (DL) dalam deteksi penipuan kartu kredit telah memberikan dampak positif yang signifikan bagi industri keuangan. Teknologi ini tidak hanya mengurangi kerugian keuangan dengan mendeteksi dan mencegah aktivitas penipuan secara real-time dengan lebih cepat dan akurat, tetapi juga meningkatkan kepercayaan pelanggan dan institusi terhadap keamanan sistem keuangan. Peningkatan akurasi deteksi dan kemampuan untuk belajar dari pola penipuan yang berkembang secara terus-menerus merupakan faktor kunci dalam memberikan perlindungan yang lebih efektif. Selain itu, kemampuan ML dan DL untuk beradaptasi dengan skema penipuan yang semakin canggih memastikan bahwa sistem deteksi tidak hanya efektif untuk saat ini, tetapi juga siap menghadapi tantangan masa depan. Dengan demikian, implementasi teknologi ML dan DL tidak hanya memperkuat keamanan transaksi keuangan saat ini tetapi juga menjaga keandalan jangka panjang dalam menghadapi ancaman keamanan yang terus berkembang.

KESIMPULAN DAN KETERBATASAN

Bagian ini berisi kesimpulan penelitian, keterbatasan penelitian, dan saran untuk penelitian kedepannya.

Kesimpulan

Penerapan machine learning (ML) dan deep learning (DL) dalam deteksi penipuan kartu kredit, temuan menunjukkan bahwa kedua teknologi ini memiliki dampak signifikan dalam meningkatkan keakuratan dan efisiensi deteksi penipuan. Penggunaan ML dan DL telah terbukti mampu mengidentifikasi pola-pola penipuan yang kompleks dan sulit dideteksi oleh metode tradisional. Algoritma-algoritma seperti Random Forest, XGBoost, dan Convolutional Neural Network (CNN), LSTM, dan beberapa lainnya menunjukkan kinerja yang sangat baik dalam mengklasifikasikan transaksi kartu kredit sebagai sah atau curang, dengan tingkat akurasi yang tinggi dan kemampuan adaptasi terhadap pola penipuan yang semakin berkembang. Selain itu, integrasi antar algoritma juga menunjukkan potensi untuk meningkatkan kinerja sistem secara keseluruhan, menggabungkan kekuatan masing-masing algoritma untuk mengatasi kelemahan yang ada.

Implementasi ML dan DL tidak hanya mengurangi risiko keuangan akibat penipuan tetapi juga meningkatkan kepercayaan pelanggan terhadap sistem keuangan secara keseluruhan. Hal ini menggambarkan bahwa penggunaan teknologi canggih dalam deteksi penipuan kartu kredit tidak hanya menjadi pilihan, tetapi kebutuhan mendesak dalam menjaga keamanan dan integritas transaksi finansial di era digital ini yang semakin rumit.

Keterbatasan

Penelitian ini memiliki keterbatasan terkait aksesibilitas literatur, karena tidak semua artikel yang diterbitkan dalam jurnal yang terindeks oleh Scopus dapat diakses secara bebas. Keterbatasan ini berpotensi mengurangi cakupan dan kedalaman analisis, mengingat bahwa beberapa temuan penting atau perkembangan terbaru dalam bidang deteksi penipuan kartu kredit mungkin tidak terjangkau. Hal ini memberi dampak pada kemampuan untuk melakukan tinjauan literatur yang komprehensif dan menyeluruh

Rekomendasi

Rekomendasi yang diberikan peneliti untuk masa mendatang yaitu untuk terus mengembangkan dan mengintegrasi berbagai algoritma dalam mendeteksi penipuan kartu kredit dengan memperhatikan karakteristik dan kebutuhan data. Selanjutnya dapat mengeksplorasi kombinasi yang lebih beragam dan inovatif, seperti menggabungkan teknik *deep learning* dengan metode pembelajaran tradisional seperti DNN dan NB. Selain itu, peneliti dapat bekerja sama dengan industri untuk mengakses data *real-world* yang lebih komprehensif dan bervariasi, serta menerapkan model yang dikembangkan dalam lingkungan produksi untuk menguji efektivitasnya.

REFERENSI

Abdul Salam, M., Fouad, K. M., Elbably, D. L., & Elsayed, S. M. (2024). Federated learning model for credit card fraud detection with data balancing techniques. *Neural Computing and Applications*, *36*(11), 6231–6256. https://doi.org/10.1007/s00521-023-09410-2

Ahmad, H., Kasasbeh, B., Aldabaybah, B., & Rawashdeh, E. (2023). Class balancing framework for credit card fraud detection based on clustering and similarity-based selection (SBS). *International Journal of Information Technology (Singapore)*, *15*(1), 325–333. https://doi.org/10.1007/s41870-022-00987-w

Ahmad Wani, T., & Wajid Ali, S. (2015). Innovation Difusion heory Review & Scope in the Study of Adoption of Smartphones in India Journal of General Management. *Journal of General Management Research*, *3*, 101–118.

Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review. In *Applied Sciences (Switzerland)* (Vol. 12, Issue 19). MDPI. https://doi.org/10.3390/app12199637

Almhaithawi, D., Jafar, A., & Aljnidi, M. (2020). Example-dependent cost-sensitive credit cards fraud detection using SMOTE and Bayes minimum risk. *SN Applied Sciences*, *2*(9). https://doi.org/10.1007/s42452-020-03375-w

Alshawi, B. (2023). Utilizing GANs for Credit Card Fraud Detection: A Comparison of Supervised Learning Algorithms. *Engineering, Technology and Applied Science Research*, *13*(6), 12264–12270. https://doi.org/10.48084/etasr.6434

Azim Mim, M., Majadi, N., & Mazumder, P. (2024). A soft voting ensemble learning approach for credit card fraud detection. *Heliyon*, *10*(3). https://doi.org/10.1016/j.heliyon.2024.e25466

Baker, M. R., Mahmood, Z. N., & Shaker, E. H. (2022). Ensemble Learning with Supervised Machine Learning Models to Predict Credit Card Fraud Transactions. *Revue d'Intelligence Artificielle*, *36*(4), 509–518. https://doi.org/10.18280/ria.360401

Balasupramanian, N., Ephrem, B. G., & Al-Barwani, I. S. (2017). User pattern based online fraud detection and prevention using big data analytics and self organizing maps. *2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, 691–694.

Benchaji, I., Douzi, S., El Ouahidi, B., & Jaafari, J. (2021). Enhanced credit card fraud detection based on attention mechanism and LSTM deep model. *Journal of Big Data*, *8*(1). https://doi.org/10.1186/s40537-021-00541-8

Btoush, E. A. L. M., Zhou, X., Gururajan, R., Chan, K. C., Genrich, R., & Sankaran, P. (2023). A systematic review of literature on credit card cyber fraud detection using machine and deep learning. *PeerJ Computer Science*, *9*. https://doi.org/10.7717/PEERJ-CS.1278

Carneiro, E. M., Forster, C. H. Q., Mialaret, L. F. S., Dias, L. A. V., & da Cunha, A. M. (2022). High-Cardinality Categorical Attributes and Credit Card Fraud Detection. *Mathematics*, *10*(20). https://doi.org/10.3390/math10203808

Chaudhary, K., Yadav, J., & Mallick, B. (2012). A review of Fraud Detection Techniques: Credit Card. In *International Journal of Computer Applications* (Vol. 45, Issue 1).

Cherif, A., Badhib, A., Ammar, H., Alshehri, S., Kalkatawi, M., & Imine, A. (2023). Credit card fraud detection in the era of disruptive technologies: A systematic review. In *Journal of King Saud University - Computer and Information Sciences* (Vol. 35, Issue 1, pp. 145–174). King Saud bin Abdulaziz University. https://doi.org/10.1016/j.jksuci.2022.11.008

Du, H. C., Lv, L., Wang, H., & Guo, A. (2024). A novel method for detecting credit card fraud problems. *PLoS ONE*, *19*(3 March). https://doi.org/10.1371/journal.pone.0294537

Du, H., Lv, L., Guo, A., & Wang, H. (2023). AutoEncoder and LightGBM for Credit Card Fraud Detection Problems. *Symmetry*, *15*(4). https://doi.org/10.3390/sym15040870

García-Avilés, J. A. (2020). Diffusion of Innovation. In *The International Encyclopedia of Media Psychology* (pp. 1–8). Wiley. https://doi.org/10.1002/9781119011071.iemp0137

Gwale, D., & Sharma, S. (2023). Issue 7 www.jetir.org (ISSN-2349-5162). In *JETIR2307462 Journal of Emerging Technologies and Innovative Research* (Vol. 10). www.jetir.org

Herland, M., Khoshgoftaar, T. M., & Bauder, R. A. (2018). Big Data fraud detection using multiple medicare data sources. *Journal of Big Data*, *5*(1). https://doi.org/10.1186/s40537-018-0138-3

Hoang Khang, V., Tung Anh, C., Dinh Thuan, N., & Chi Minh City, H. (n.d.). Detecting Fraud Transaction using Ripper Algorithm Combines with Ensemble Learning Model. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 14, Issue 4). www.ijacsa.thesai.org

Hussein, A. S., Khairy, R. S., Mohamed Najeeb, S. M., & Salim ALRikabi, H. T. (2021). Credit Card Fraud Detection Using Fuzzy Rough Nearest Neighbor and Sequential Minimal Optimization with Logistic Regression. *International Journal of Interactive Mobile Technologies*, *15*(5), 24–42. https://doi.org/10.3991/ijim.v15i05.17173

Ileberi, E., Sun, Y., & Wang, Z. (2021). Performance Evaluation of Machine Learning Methods for Credit Card Fraud Detection Using SMOTE and AdaBoost. *IEEE Access*, *9*, 165286–165294. https://doi.org/10.1109/ACCESS.2021.3134330

Ingole, P., Wagh, N., Nandanwar, S., Bharsakale, R., & Raut, J. (2023). Literature Review On Identification Of Fraudulent Credit Card Fraud Detection Using Deep Learning. In *International Journal of Creative Research Thoughts* (Vol. 11). www.ijcrt.org

Jayanthi, E., Ramesh, T., Kharat, R. S., Veeramanickam, M. R. M., Bharathiraja, N., Venkatesan, R., & Marappan, R. (2023). Cybersecurity enhancement to detect credit card frauds in health care using new machine learning strategies. *Soft Computing*, *27*(11), 7555–7565. https://doi.org/10.1007/s00500-023-07954-y

Jha, B. K., Sivasankari, G. G., & Venugopal, K. R. (2020). Fraud Detection and Prevention by using Big Data Analytics. *Proceedings of the 4th International Conference on Computing Methodologies and Communication, ICCMC 2020*, 267–274. https://doi.org/10.1109/ICCMC48092.2020.ICCMC-00050

Malik, E. F., Khaw, K. W., Belaton, B., Wong, W. P., & Chew, X. (2022). Credit Card Fraud Detection Using a New Hybrid Machine Learning Architecture. *Mathematics*, *10*(9). https://doi.org/10.3390/math10091480

Moh. Badris Sholeh Rahmatullah, Aulia Ligar Salma Hanani, Akmal Muhammad Naim, Zamah Sari, & Yufis Azhar. (2022). Detection of Credit Card Fraud with Machine Learning Methods and Resampling Techniques. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *6*(6), 923–929. https://doi.org/10.29207/resti.v6i6.4213

Mqadi, N., Naicker, N., & Adeliyi, T. (2021). A SMOTe based oversampling data-point approach to solving the credit card data imbalance problem in financial fraud detection. *International Journal of Computing and Digital Systems*, *10*(1), 277–286. https://doi.org/10.12785/IJCDS/100128

Ningsih, P. T. S., Gusvarizon, M., & Hermawan, R. (2022). Analisis Sistem Pendeteksi Penipuan Transaksi Kartu Kredit dengan Algoritma Machine Learning. *Jurnal Teknologi Informatika Dan Komputer*, *8*(2), 386–401.

Pandey, N., Rani, S. B., Student, B., & Asst Professor, S. (2018). *CREDIT CARD FRAUD DETECTION USING BIG DATA FRAMEWORK* (Vol. 6, Issue 2). www.ijcrt.org

Paruchuri, H. (2017). Credit Card Fraud Detection using Machine Learning: A Systematic Literature Review. In *ABC Journal of Advanced Research* (Vol. 6, Issue 2).

Razaque, A., Frej, M. B. H., Bektemyssova, G., Amsaad, F., Almiani, M., Alotaibi, A., Jhanjhi, N. Z., Amanzholova, S., & Alshammari, M. (2023). Credit Card-Not-Present Fraud Detection and Prevention Using Big Data Analytics Algorithms. *Applied Sciences (Switzerland)*, *13*(1). https://doi.org/10.3390/app13010057

Roy, A., Sun, J., Mahoney, R., Alonzi, L., Adams, S., & Beling, P. (2018). Deep learning detecting fraud in credit card transactions. *2018 Systems and Information Engineering Design Symposium (SIEDS)*, 129–134. https://doi.org/10.1109/SIEDS.2018.8374722

Sharma, P., Banerjee, S., Tiwari, D., & Patni, J. C. (2021). Machine learning model for credit card fraud detection-A comparative analysis. *International Arab Journal of Information Technology*, *18*(6), 789–796. https://doi.org/10.34028/iajit/18/6/6

Shinde, P. P., & Shah, S. (2018). A Review of Machine Learning and Deep Learning Applications. *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, 1–6. https://doi.org/10.1109/ICCUBEA.2018.8697857

Slabber, E., Verster, T., & de Jongh, R. (2023). Some Insights about the Applicability of Logistic Factorisation Machines in Banking. *Risks*, *11*(3). https://doi.org/10.3390/risks11030048

Syahputra, B. E., & Afnan, A. (2020). Pendeteksian Fraud: Peran Big Data dan Audit Forensik. *Jurnal ASET (Akuntansi Riset)*, *12*(2), 301–316. https://doi.org/10.17509/jaset.v12i2.28939

V S S, L. S., & Deepthi Kavila, S. (2018). Machine Learning For Credit Card Fraud Detection System. In *International Journal of Applied Engineering Research* (Vol. 13). http://www.ripublication.com

Zhao, X., & Guan, S. (2023). CTCN: a novel credit card fraud detection method based on Conditional Tabular Generative Adversarial Networks and Temporal Convolutional Network. *PeerJ Computer Science*, *9*. https://doi.org/10.7717/PEERJ-CS.1634