

**JIMT:**
Jurnal Ilmu Manajemen Terapan

E-ISSN: 2686-4924
P-ISSN: 2686-5246

 <https://dinastirev.org/JIMT>  dinasti.info@gmail.com  +62 811 7404 455

DOI: <https://doi.org/10.38035/jimt.v7i3>
<https://creativecommons.org/licenses/by/4.0/>

Fraud di Sektor Perbankan: Analisis Bibliometrik atas Tren Penelitian Global

Sabna Ainazah Fatikhah¹, Ledy Yolanda², Muhammad Karisma Alam³, Deane Rahmamita⁴

¹Universitas Terbuka, Tangerang Selatan, Indonesia, sabna.ainazah@ecampus.ut.ac.id

²Universitas Terbuka, Tangerang Selatan, Indonesia, ledy.yolanda@ecampus.ut.ac.id

³Universitas Terbuka, Tangerang Selatan, Indonesia, muhammad.karisma@ecampus.ut.ac.id

⁴Universitas Terbuka, Tangerang Selatan, Indonesia, deane.rahmamita@ecampus.ut.ac.id

Corresponding Author: sabna.ainazah@ecampus.ut.ac.id¹

Abstract: *Purpose – This study aims to analyze publication trends and citation patterns in the global literature on fraud in the banking sector, identify the most influential authors, journals, and institutions, and map the main themes and emerging directions of research in this field. Design/methodology/approach – A bibliometric approach was employed to examine 137 scholarly publications indexed in the Scopus database. The analysis was conducted using VOSviewer to identify patterns of author collaboration, co-citation networks, and dominant keyword clusters within the body of research on banking fraud. Findings – The results reveal a significant surge in both publications and citations since 2020, likely driven by the increasing complexity of digital financial systems and the need for strengthened regulatory frameworks in the post-pandemic context. The findings indicate that fraud in the banking sector has become an issue of growing global concern, with research increasingly focusing on fraud detection technologies, regulatory oversight, risk management, and the role of artificial intelligence and big data in fraud prevention. Originality/value – This study provides a comprehensive bibliometric mapping of research on fraud in the banking sector. It offers strategic insights for scholars and policymakers to better understand global research trajectories and identify existing research gaps. Practical implications – From a policy perspective, the study underscores the importance of strengthening financial supervisory systems, fostering cross-sector collaboration, and investing in adaptive, real-time fraud detection technologies. Social implications – The study highlights the critical role of public trust in the banking system and consumer protection in fostering a stable, transparent, and sustainable financial ecosystem.*

Keyword: *Fraud, Banking, Bibliometric analysis, Financial crime, Regulation*

Abstrak: Tujuan – Penelitian ini bertujuan untuk menganalisis tren publikasi dan pola kutipan dalam kajian global terkait fraud (kecurangan) di sektor perbankan, mengidentifikasi penulis, jurnal, dan institusi paling berpengaruh, serta memetakan tema-tema utama dan arah perkembangan riset dalam bidang ini. Desain/metodologi/pendekatan – Penelitian ini menggunakan pendekatan bibliometrik terhadap 137 publikasi ilmiah yang terindeks di basis data Scopus. Analisis dilakukan dengan bantuan perangkat lunak VOSviewer untuk

mengidentifikasi kolaborasi penulis, jaringan ko-sitasi, serta kluster kata kunci yang dominan dalam penelitian tentang fraud di sektor perbankan. Temuan – Hasil studi menunjukkan lonjakan signifikan dalam jumlah publikasi dan sitasi sejak tahun 2020, yang kemungkinan dipicu oleh meningkatnya kompleksitas sistem keuangan digital dan kebutuhan akan penguatan regulasi pasca-pandemi. Temuan utama mengindikasikan bahwa isu fraud dalam perbankan semakin menjadi perhatian global, dengan fokus pada teknologi deteksi penipuan, pengawasan regulasi, manajemen risiko, serta peran kecerdasan buatan dan big data dalam pencegahan fraud. Orisinalitas/nilai – Studi ini menyajikan pemetaan bibliometrik yang komprehensif mengenai penelitian fraud di sektor perbankan. Analisis ini memberikan wawasan strategis bagi peneliti dan pembuat kebijakan untuk memahami arah riset global serta mengidentifikasi celah penelitian yang masih terbuka. Implikasi – Dari sisi kebijakan, penelitian ini menekankan pentingnya penguatan sistem pengawasan keuangan, kolaborasi lintas sektor, serta investasi dalam teknologi pendeteksian fraud yang adaptif dan real-time. Implikasi sosial – Kajian ini menyoroti pentingnya kepercayaan publik terhadap sistem perbankan dan perlindungan konsumen dalam menciptakan ekosistem keuangan yang stabil, transparan, dan berkelanjutan.

Kata Kunci: Fraud, Perbankan, Analisis bibliometrik, Kejahatan keuangan, Regulasi

PENDAHULUAN

Fraud merupakan salah satu tantangan global paling serius yang dihadapi sektor perbankan modern karena dampaknya yang tidak hanya terbatas pada kerugian finansial, tetapi juga mencakup penurunan kepercayaan publik dan gangguan terhadap stabilitas sistem keuangan. Dalam konteks perbankan, fraud mencakup berbagai bentuk penyimpangan, mulai dari pencurian aset, manipulasi transaksi, pemalsuan dokumen, pencucian uang, hingga pelaporan keuangan yang tidak benar. Secara kolektif, praktik-praktik tersebut menimbulkan kerugian ekonomi berskala besar dan berdampak luas terhadap masyarakat serta perekonomian global ((Ming et al. 2024);(Ramos et al. 2024); (Sood and Bhushan 2020). Skala permasalahan ini tercermin dari laporan Canadian Anti-Fraud Centre yang mencatat lebih dari 91.190 kasus penipuan pada tahun 2022 dengan total kerugian korban melebihi USD 531 juta. Secara global, kerugian akibat fraud diperkirakan mencapai sekitar 5% dari total pendapatan organisasi setiap tahun, dengan estimasi hampir USD 4 triliun, sehingga menjadikan fraud sebagai risiko sistemik bagi keberlanjutan organisasi dan stabilitas ekonomi dunia (Gepp et al. 2018).

Sektor perbankan menjadi target utama pelaku fraud karena karakteristiknya yang sangat bergantung pada transaksi keuangan, sistem informasi, dan tingkat kepercayaan publik yang tinggi. Dampak fraud terhadap perbankan tidak hanya berupa kerugian finansial langsung, tetapi juga penurunan profitabilitas, melemahnya kapasitas investasi, serta terganggunya fungsi intermediasi bank dalam menyalurkan kredit kepada sektor riil. Kondisi ini berpotensi memperlambat pertumbuhan ekonomi dan meningkatkan ketidakstabilan sistem keuangan. Lebih lanjut, meningkatnya kasus fraud dapat menurunkan kepercayaan masyarakat terhadap institusi perbankan, menghambat adopsi layanan keuangan digital, serta melemahkan upaya pemerintah dalam mendorong inklusi keuangan sebagai instrumen pembangunan ekonomi berkelanjutan ((Odufisan, Abhulimen, and Ogunti 2025); (Sharma, Sharma, and Aggarwal 2020).

Transformasi digital dalam sektor perbankan telah mempercepat integrasi teknologi informasi melalui perbankan daring, mobile banking, dan sistem pembayaran digital. Meskipun digitalisasi meningkatkan efisiensi dan aksesibilitas layanan, perkembangan ini juga memunculkan risiko baru berupa lonjakan kejahatan siber. Pelaku fraud memanfaatkan kelemahan sistem perbankan digital melalui teknik phishing, malware, pencurian identitas, dan rekayasa sosial untuk memperoleh akses tidak sah terhadap data dan aset keuangan nasabah (Swati Gupta 2025). Dengan demikian, digitalisasi perbankan dapat dipandang sebagai pisau

bermata dua, di mana inovasi layanan berjalan beriringan dengan meningkatnya kompleksitas dan skala risiko fraud (AbouGrad and Sankuru 2025).

Seiring meningkatnya kompleksitas fraud, perhatian akademik terhadap isu ini juga menunjukkan pertumbuhan yang signifikan, terutama sejak krisis keuangan global 2008–2009 yang mengungkap berbagai kelemahan struktural dalam sistem keuangan internasional. Penelitian global mengenai fraud di sektor perbankan menunjukkan tren peningkatan yang tajam, dengan fokus dominan pada fraud kartu kredit dan fraud transaksi digital. Dominasi topik ini sebagian besar didorong oleh ketersediaan dataset publik yang memungkinkan pengembangan dan pengujian model deteksi fraud berbasis kecerdasan buatan dan machine learning (Moro, Cortez, and Rita 2015); (Chen et al. 2025). Namun demikian, literatur yang ada masih menunjukkan ketimpangan fokus penelitian, di mana jenis fraud lain seperti mortgage fraud, pencucian uang, dan penipuan sekuritas relatif kurang mendapat perhatian dibandingkan fraud kredit dan kartu pembayaran (Moro et al. 2015).

Perkembangan teknologi digital juga mendorong transformasi metodologi dalam penelitian dan praktik deteksi fraud perbankan. Penerapan big data analytics (BDA), artificial intelligence (AI), dan machine learning (ML) memungkinkan analisis data berskala besar secara real-time, peningkatan akurasi prediksi risiko, serta efisiensi operasional dalam sistem perbankan (Owusu 2025); (Byrapu Reddy et al. 2024); (Singh et al. 2022). Berbagai pendekatan deep learning, seperti multilayer perceptron (MLP), convolutional neural network (CNN), dan long short-term memory (LSTM), telah menunjukkan tingkat akurasi yang sangat tinggi dalam mendeteksi transaksi fraud, bahkan melebihi 97% pada dataset tertentu (Khan et al. 2025). Selain itu, metode lain seperti Pattern Recognition K-Nearest Neighbor (PR-KNN) dan algoritma optimasi terus dikembangkan untuk meningkatkan presisi deteksi dan mengurangi tingkat false alarm (Kannagi et al. 2021).

Meskipun demikian, kemajuan teknologi ini belum sepenuhnya mampu mengatasi berbagai tantangan mendasar dalam penelitian fraud. Permasalahan seperti ketidakseimbangan data, keterbatasan generalisasi model, kurangnya validasi lintas konteks, serta kebutuhan akan pendekatan yang lebih berorientasi pada pengguna masih menjadi isu utama dalam literatur terkini (Khan et al. 2025). Oleh karena itu, penelitian masa depan diharapkan tidak hanya berfokus pada pengembangan algoritma deteksi, tetapi juga mengadopsi pendekatan multidisipliner yang mengintegrasikan big data, analisis perilaku, serta faktor psikologis dan organisasi yang melatarbelakangi terjadinya fraud (Nguyen et al., 2022; Cumming, Dannhauser, & Johan, 2015).

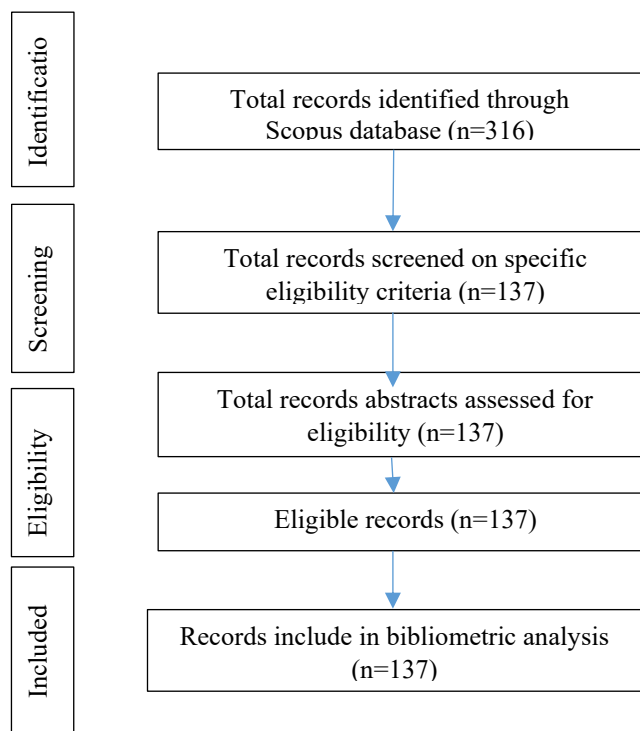
Dalam konteks tersebut, studi bibliometrik menjadi pendekatan yang relevan dan strategis untuk memetakan perkembangan penelitian fraud di sektor perbankan secara global. Analisis bibliometrik memungkinkan identifikasi tren publikasi, struktur sitasi, aktor dan kolaborasi ilmiah, topik dominan, serta kesenjangan penelitian yang masih terbuka. Dengan demikian, penelitian ini diharapkan dapat memberikan wawasan komprehensif mengenai dinamika riset fraud perbankan, sekaligus menjadi dasar bagi pengembangan agenda penelitian di masa depan yang lebih terarah dalam mendukung sistem perbankan yang aman, terpercaya, dan berkelanjutan ((Odufisan et al. 2025); (Chen et al. 2025); (Moro et al. 2015); (Khan et al. 2025); (Singh et al. 2022).

Tujuan dari kajian ini adalah untuk (RQ1) menganalisis tren dalam volume publikasi dan struktur kutipan dalam korpus penelitian tentang fraud di sektor perbankan. (RQ2) mengidentifikasi kontributor paling aktif dalam domain ini, termasuk jurnal dan artikel paling berpengaruh; (RQ3) memetakan struktur intelektual dan sosial dari literatur tentang fraud di sektor perbankan; (RQ4) meneliti apa saja strategi, kebijakan dan teknologi yang direkomendasikan dalam literatur untuk mengurangi dan mencegah fraud di sektor perbankan dan (RQ5) Apa saja tema-tema yang muncul dan arah penelitian di masa depan tentang fraud di sektor perbankan. Temuan dari analisis ini diharapkan dapat memberikan kontribusi pada pemahaman yang lebih mendalam tentang perkembangan penelitian global terkait fraud di

sektor perbankan, termasuk tren, pendekatan, dan strategi penanggulangannya. Hasil kajian ini juga bertujuan memberikan rekomendasi untuk mendukung perumusan kebijakan dan implementasi praktik keamanan perbankan yang lebih efektif dalam mencegah dan mendeteksi tindakan fraud. Selain itu, temuan ini dapat menjadi landasan penting bagi peneliti, regulator, dan praktisi industri perbankan dalam merancang strategi berkelanjutan guna memperkuat integritas sistem keuangan dan meningkatkan kepercayaan publik di tengah kemajuan teknologi dan kompleksitas risiko kejahatan keuangan yang terus berkembang.

METODE

Studi ini mengadopsi analisis bibliometrik untuk mengungkap tren global dalam penelitian tentang fraud di sektor perbankan. Strategi pencarian dirancang menggunakan kombinasi kata kunci yang terkait dengan "bank fraud" OR "banking fraud" OR "fraud in banking sector" OR "fraudulent banking activities" OR "bank fraud detection" OR "banking scam" OR "bank insider fraud" OR "bank embezzlement" dengan operator Boolean, dibatasi pada judul, abstrak, dan kata kunci artikel berbahasa Inggris yang diterbitkan antara tahun 2015 dan 2025. Hingga 19 Januari 2025, pencarian menghasilkan set awal yang terdiri dari 316 dokumen.



Sumber: Elaborasi penulis
Gambar 1. Desain Penelitian

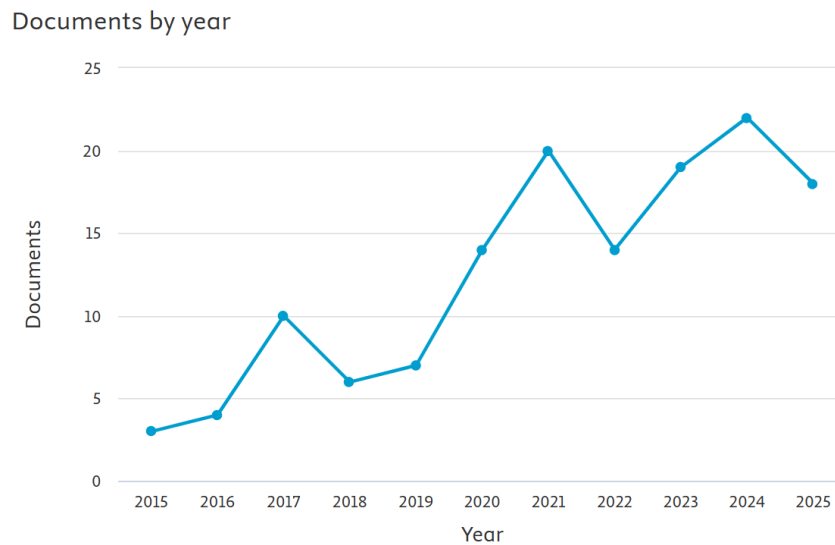
Melalui proses seleksi yang ketat, 179 dokumen dianggap tidak relevan, sehingga menyisakan 137 publikasi yang memenuhi kriteria. Analisis bibliometrik mempertimbangkan tahun publikasi, sumber jurnal, afiliasi institusi, negara asal, dan jumlah kutipan untuk memetakan tren penelitian, pola publikasi, dan jaringan kolaborasi. Pendekatan ini tidak hanya menggambarkan dinamika penelitian tentang fraud (kecurangan) di sektor perbankan tetapi juga memberikan wawasan tentang arah penelitian di masa mendatang dan area potensial yang belum dieksplorasi.

HASIL DAN PEMBAHASAN

Analisis kinerja

Analisis Tren Publikasi. Tren publikasi kronologis yang ditampilkan dalam Gambar 2 mengilustrasikan analisis tren tahunan volume dan dampak (RQ1) dari korpus penelitian

mengenai fraud di sektor perbankan sepanjang tahun 2015 hingga 2024. Analisis ini menyoroti fluktuasi signifikan dalam jumlah publikasi, yang mencerminkan dinamika perhatian akademis terhadap isu kejahatan keuangan dan tantangan yang dihadapi sistem perbankan global.



Sumber: Scopus, 2025

Gambar 2. Tren penelitian tentang fraud di sektor perbankan

Tren penelitian mengenai fraud di sektor perbankan menunjukkan pola pertumbuhan jangka panjang yang jelas, meskipun disertai fluktuasi pada beberapa tahun tertentu. Pada periode awal, yaitu 2015–2016, jumlah publikasi masih relatif rendah, dengan hanya sekitar 3 hingga 4 dokumen per tahun, yang mengindikasikan bahwa kajian fraud perbankan pada fase ini masih terbatas dan belum menjadi fokus utama dalam literatur akademik global.

Peningkatan mulai terlihat pada tahun 2017, ketika jumlah publikasi meningkat secara signifikan menjadi sekitar 10 dokumen, sebelum kembali mengalami penurunan pada 2018–2019 dengan kisaran 6–7 publikasi per tahun. Fluktuasi ini mencerminkan fase transisi, di mana isu fraud perbankan mulai mendapat perhatian, namun belum berkembang secara konsisten sebagai agenda riset yang mapan.

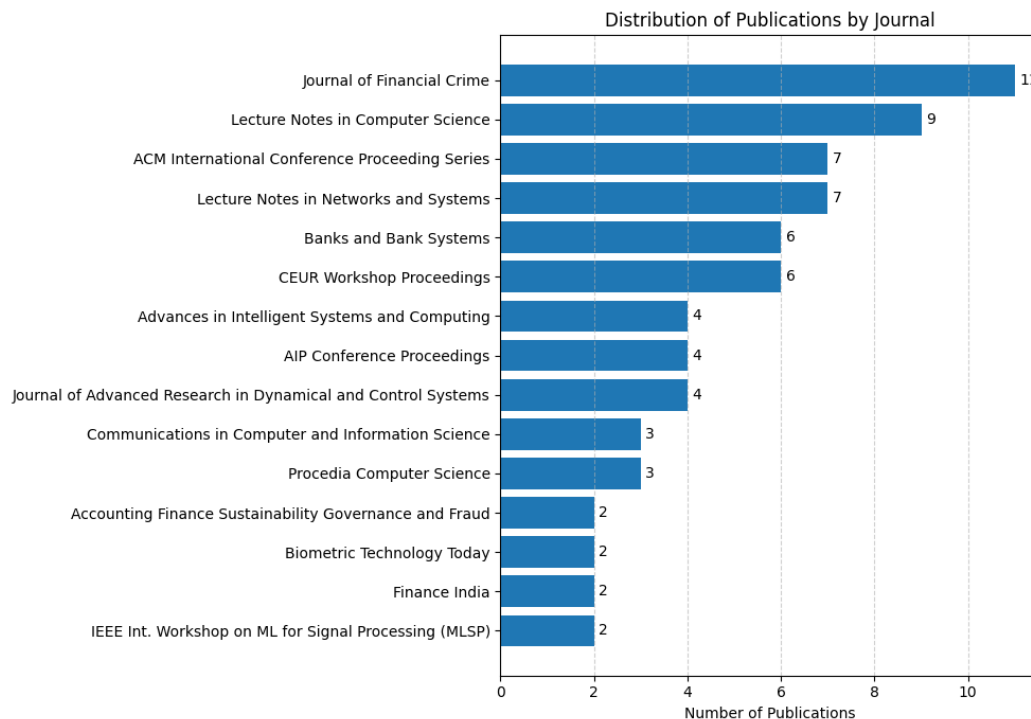
Lonjakan yang lebih kuat terjadi sejak tahun 2020, dengan jumlah publikasi meningkat menjadi sekitar 14 dokumen, dan mencapai puncak sementara pada 2021 dengan sekitar 20 publikasi. Peningkatan ini bertepatan dengan percepatan digitalisasi sistem perbankan, meningkatnya transaksi elektronik, serta eskalasi risiko kejahatan keuangan yang mendorong kebutuhan akan metode deteksi fraud yang lebih canggih, termasuk pendekatan berbasis kecerdasan buatan dan analitik data.

Meskipun terjadi penurunan pada tahun 2022 (sekitar 14 dokumen), tren penelitian kembali menunjukkan penguatan pada periode berikutnya. Jumlah publikasi meningkat kembali pada 2023 (sekitar 19 dokumen) dan mencapai titik tertinggi pada 2024 dengan sekitar 22 publikasi, sebelum mengalami sedikit penurunan pada 2025 (sekitar 18 dokumen), yang kemungkinan disebabkan oleh keterbatasan data tahun berjalan (*partial year effect*).

Secara keseluruhan, pola ini menegaskan bahwa penelitian tentang fraud di sektor perbankan berkembang secara bertahap namun berkelanjutan, dengan akselerasi yang nyata dalam lima tahun terakhir. Tren tersebut mencerminkan meningkatnya kompleksitas fraud perbankan akibat inovasi teknologi keuangan, penggunaan artificial intelligence dan machine learning, serta meningkatnya ancaman kejahatan siber. Dengan demikian, fraud perbankan semakin dipahami sebagai isu strategis lintas disiplin yang melibatkan keuangan, teknologi informasi, manajemen risiko, dan tata kelola, sekaligus menegaskan relevansinya dalam mendukung pengembangan kebijakan dan sistem pencegahan fraud yang adaptif terhadap dinamika keuangan global.

Jurnal paling terkemuka dan aktif

Analisis ini menyoroti kontributor-kontributor utama dalam domain (RQ2) yaitu jurnal yang paling menonjol dan aktif, serta artikel-artikel yang paling berpengaruh akan diidentifikasi dalam analisis ini (RQ2). Gambar 3 mengilustrasikan 15 jurnal teratas berdasarkan jumlah dokumen yang diterbitkan, yang memberikan wawasan mengenai platform-platform terkemuka untuk penyebaran penelitian dalam bidang ini.



Sumber: Scopus, 2025

Gambar 3. 15 Jurnal Teratas Berdasarkan Jumlah Dokumen

Analisis terhadap 15 jurnal dan prosiding dengan jumlah publikasi tertinggi menunjukkan bahwa penelitian tentang fraud di sektor perbankan berkembang melalui spektrum pendekatan yang luas, mencakup dimensi keuangan, teknologi, regulasi, dan perilaku organisasi. Dominasi *Journal of Financial Crime* sebagai sumber publikasi terbanyak menegaskan bahwa kajian fraud perbankan masih berakar kuat pada perspektif kriminologi keuangan, tata kelola, serta mekanisme pengendalian dan kepatuhan dalam institusi perbankan.

Sementara itu, kontribusi signifikan dari *Lecture Notes in Computer Science*, *ACM International Conference Proceeding Series*, serta *Lecture Notes in Networks and Systems* mengindikasikan meningkatnya orientasi teknologi dalam riset fraud perbankan. Publikasi dalam sumber-sumber ini secara konsisten menyoroti pemanfaatan kecerdasan buatan, machine learning, data mining, dan sistem jaringan untuk mendeteksi pola transaksi mencurigakan, mengidentifikasi anomali, serta meningkatkan efektivitas sistem pencegahan fraud di lingkungan perbankan digital.

Jurnal dan prosiding seperti *Banks and Bank Systems*, *CEUR Workshop Proceedings*, dan *Advances in Intelligent Systems and Computing* menekankan pendekatan sistemik dan integratif, dengan fokus pada desain arsitektur sistem deteksi fraud, penguatan manajemen risiko, serta adaptasi institusi perbankan terhadap kompleksitas ancaman kejahatan finansial. Pendekatan ini mencerminkan pergeseran dari metode deteksi konvensional menuju model prediktif dan berbasis data besar.

Di sisi lain, sumber-sumber yang lebih spesifik secara teknologi, seperti *Biometric Technology Today*, *IEEE International Workshop on Machine Learning for Signal Processing (MLSP)*, dan *Communications in Computer and Information Science*, menyoroti penggunaan

verifikasi biometrik, algoritma pemrosesan sinyal, dan analisis perilaku digital untuk meningkatkan akurasi dan keandalan sistem deteksi fraud. Kehadiran jurnal-jurnal ini menunjukkan meningkatnya perhatian terhadap fraud yang berbasis identitas dan teknologi canggih, khususnya dalam konteks perbankan berbasis elektronik dan mobile banking.

Secara keseluruhan, distribusi publikasi pada 15 sumber utama ini mengonfirmasi bahwa fraud di sektor perbankan semakin dipahami sebagai tantangan multidimensi dan lintas disiplin, yang menuntut kolaborasi antara bidang keuangan, ilmu komputer, teknologi informasi, dan tata kelola organisasi. Dominasi jurnal teknologi dan keuangan dalam lanskap publikasi global menegaskan pentingnya pendekatan interdisipliner dalam merumuskan strategi pencegahan fraud yang adaptif, proaktif, dan berbasis bukti ilmiah.

Temuan ini memperkuat urgensi pengembangan kebijakan dan sistem pengawasan perbankan yang tidak hanya berfokus pada kepatuhan regulatif, tetapi juga mendorong inovasi teknologi, peningkatan kapasitas deteksi dini, serta penguatan keamanan sistem perbankan guna menciptakan ekosistem keuangan yang aman, transparan, dan berkelanjutan.

Analisis ko-sitasi

Karya-karya yang sering disitasi umumnya mencerminkan kontribusi penting dan pengaruh yang kuat terhadap perkembangan bidang keilmuan tertentu. Dalam konteks penelitian fraud di sektor perbankan, studi-studi yang paling banyak dikutip menunjukkan landasan teoretis dan metodologis yang menjadi rujukan utama dalam memahami, mendeteksi, dan mencegah praktik kejahatan finansial

Analisis ko-sitasi

Karya-karya yang sering disitasi umumnya mencerminkan kontribusi penting dan pengaruh yang kuat terhadap perkembangan bidang keilmuan tertentu. Dalam konteks penelitian fraud di sektor perbankan, studi-studi yang paling banyak dikutip menunjukkan landasan teoretis dan metodologis yang menjadi rujukan utama dalam memahami, mendeteksi, dan mencegah praktik kejahatan finansial

Tabel 1. Analisis ko-sitasi

Penulis	Judul	Tahun	Judul Sumber	Kutip	Penerbit
(Jianmu Ye 1 and Khaled Gubran Al-Hashedi, Pritheega Magalingam, 2021)	Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019	2021	Computer Science Review	246	Elsevier
(Abdulsalam O. Alzahrani and Mohammed J. F. Alenazi, 2021)	Designing a Network Intrusion Detection System Based on Machine Learning for Software Defined Networks	2021	Future Internet	213	MDPI
(G. Logeswari, S. Bose and T. Anitha, 2023)	An Intrusion Detection System for SDN Using Machine Learning	2023	Intelligent Automation and Soft Computing,	77	Tech Science Press
(Anthony Abio Kashish A. Shakil, Farhana J. Zareen, Mansaf Alam, Suraiya Jabin, 2020)	BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud	2020	Computer and Information Sciences	77	Journal of King Saud University

Penulis	Judul	Tahun	Judul Sumber	Kutip	Penerbit
(Carminati, Michele Caron, Roberto Maggi, Federico Epifani, Ilenia Zanero, Stefano, 2015)	BankSealer: A decision support system for online banking fraud analysis and investigation	2015	Computers and Security	76	Scient Direct, Elsevier
(Ahmad Firdaus, Nor Badrul Anuar, Ahmad Karim, Mohd Faizal Ab Razak, 2018)	Discovering optimal features using static analysis and a genetic search based method for Android malware detection	2018	Frontiers of Information Technology & Electronic Engineering	70	FITEE
(Paolo Vanini, , Sebastiano Rossi, , Ermin Zvizdic and Thomas Domenig, 2023)	Online payment fraud: from anomaly detection to risk management	2023	Financial Innovation	68	Springer Open
(Douglas Cirqueira , Dietmar Nedbal, Markus Helfert , and Marija Bezbradica, 2020)	Scenario-Based Requirements Elicitation for User-Centric Explainable AI A Case in Fraud Detection	2020	Lecture Notes in Computer Science	59	Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)
(Jurjen Jansen & Rutger Leukfeldt, 2016)	Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization	2016	International Journal of Cyber Criminology	58	International Journal of Cyber Criminology
<u>Nana Kwame Gyamfi, Jamal-Deen Abdulai,</u>	Bank Fraud Detection Using Support Vector Machine	2018	IEEE	72	2018 IEEE 9th Annual Information Technology Electronics and Mobile Communication Conference Iemcon 2018, pp. 37–41, 8614994

Sumber : Karya penulis sendiri, 2025

Tabel 1 mencerminkan tren penelitian global terkait fraud di sektor perbankan, dengan pendekatan lintas disiplin yang mencakup ilmu komputer, keamanan siber, kecerdasan buatan, dan sistem keuangan digital. Studi oleh (Al-Hashedi and Magalingam 2021) menjadi yang paling banyak dikutip (246 kutipan), menyoroti evolusi teknik data mining dalam deteksi fraud finansial selama satu dekade terakhir. Karya ini menjadi referensi utama dalam mengidentifikasi pola fraud berdasarkan pendekatan berbasis data.

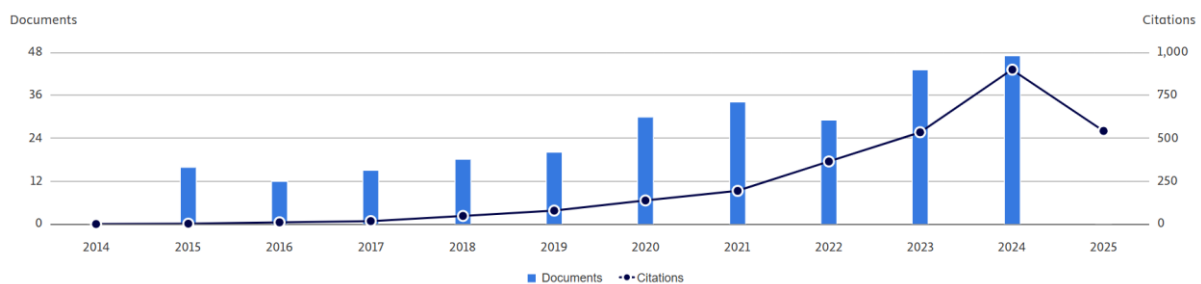
Sementara itu, studi oleh (Alzahrani and Alenazi 2021) yang mengembangkan sistem deteksi intrusi berbasis machine learning untuk jaringan software-defined (SDN), juga menjadi acuan penting dengan 213 kutipan, menandakan meningkatnya integrasi antara teknologi jaringan dan sistem deteksi kejahatan keuangan. Demikian pula, (Logeswari, Bose, and Anitha 2023) dan (Shakil et al. 2020) mengeksplorasi pendekatan baru dalam sistem keamanan dan otentikasi berbasis biometrik serta cloud computing, yang semakin relevan dengan infrastruktur perbankan modern.

Studi klasik seperti (Carminati et al. 2015) yang dikutip 76 kali, memberikan kontribusi signifikan dalam mendukung investigasi fraud perbankan secara online melalui sistem pendukung keputusan. Penelitian oleh (Vanini et al. 2023) dan (Jansen and Leukfeldt 2016) memperluas cakupan dengan membahas fraud pembayaran daring dan serangan phishing terhadap nasabah bank, menunjukkan bahwa aspek sosial dan psikologis juga menjadi perhatian utama dalam studi fraud.

Dari sisi pendekatan teknologi, studi (Firdaus et al. 2018) dan (Nana Kwame Gyamfi 2018) mengeksplorasi penggunaan algoritma kecerdasan buatan dan SVM (Support Vector Machine) dalam mendeteksi malware serta aktivitas fraud, memperlihatkan pergeseran dari pendekatan reaktif ke sistem prediktif berbasis AI.

Penerbit-penerbit besar seperti Elsevier, MDPI, Springer Open, dan IEEE menjadi rumah bagi sebagian besar publikasi ini, mencerminkan luasnya pengakuan dan cakupan global dari penelitian fraud perbankan. Secara keseluruhan, karya-karya ini menunjukkan tiga arah utama dalam penelitian yaitu Integrasi teknologi dalam deteksi fraud, Pendekatan sistemik terhadap investigasi keuangan, dan Peningkatan keamanan transaksi digital berbasis AI dan jaringan.

Temuan ini menegaskan bahwa fraud di sektor perbankan merupakan isu multidimensional yang terus berkembang, dan studi-studi terpilih dalam tabel ini telah membentuk fondasi penting bagi pengembangan sistem deteksi yang lebih adaptif, akurat, dan transparan di masa depan.



Sumber : Karya penulis sendiri, 2025
Gambar 4. Kutipan selama tahun 2015-2025

Berdasarkan grafik tren publikasi dan sitasi dari tahun 2015 hingga 2024, terlihat adanya peningkatan yang signifikan dalam jumlah dokumen dan kutipan terkait topik fraud di sektor perbankan. Pada periode awal (2015–2016), volume publikasi masih relatif rendah dan stabil, mencerminkan minimnya perhatian akademik terhadap isu ini. Namun, sejak tahun 2017 mulai terjadi peningkatan secara bertahap, baik dari jumlah dokumen yang diterbitkan maupun jumlah kutipan yang diterima.

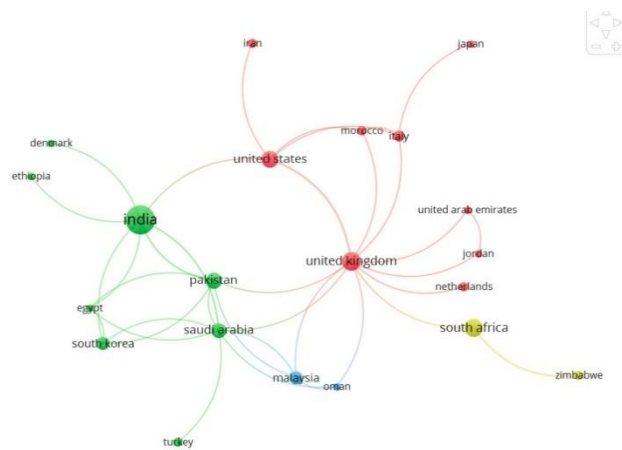
Tren pertumbuhan semakin menguat sejak tahun 2019, ketika jumlah dokumen yang dipublikasikan mulai meningkat secara konsisten setiap tahunnya. Lonjakan signifikan terjadi pada tahun 2022, dan mencapai puncaknya pada tahun 2024 dengan hampir 40 dokumen yang dipublikasikan dan lebih dari 900 sitasi yang diterima, menandakan puncak perhatian akademik terhadap topik ini. Fenomena ini mengindikasikan bahwa isu fraud dalam perbankan semakin relevan dan mendesak untuk diteliti, terutama seiring dengan meningkatnya digitalisasi layanan keuangan, kompleksitas transaksi perbankan, dan kerentanan terhadap kejahatan siber.

Kenaikan tajam dalam jumlah sitasi menunjukkan bahwa literatur di bidang ini semakin dijadikan rujukan utama oleh akademisi, regulator, dan praktisi keuangan dalam merancang kebijakan mitigasi risiko, penguatan sistem pengawasan, serta pengembangan teknologi deteksi fraud berbasis AI dan big data. Secara keseluruhan, tren ini menggarisbawahi pentingnya studi lintas disiplin dalam menghadapi dinamika dan tantangan fraud di sektor perbankan global masa kini.

Jaringan Penulisan Bersama Antar negara

Jaringan kepenulisan bersama antar negara (*co-authorship*) memetakan kolaborasi riset yang terbentuk dari lintas negara. Jaringan ini terbentuk dari *node* (simpul) yang merepresentasikan negara dan garis penghubung yang menunjukkan adanya publikasi bersama antar negara, seperti yang terlihat pada Gambar 5. Adanya perbedaan warna mengindikasikan terbentuknya beberapa klaster kolaborasi, yaitu kelompok negara yang banyak ditemukan penulisan bersama. Pada jaringan ini, negara yang berada pada posisi sentral biasanya memiliki peran utama sebagai penggerak publikasi dan penghubung arus pengetahuan antarkelompok.

Pada Gambar 5, tampak negara yang berperan sebagai penghubung yaitu India dan United Kingdom. Hal ini menunjukkan bahwa posisi dan koneksi kedua negara ini cukup strategis untuk kolaborasi internasional dalam topik ini. Selain itu, negara-negara di sekitarnya yang memiliki sedikit koneksi, yang disebut sebagai negara-negara *perifir* menunjukkan bahwa kolaborasi terkait topik ini belum merata. Struktur seperti ini menunjukkan bahwa yang pertama, konsentrasi jaringan penulis berpusat pada negara kolaborasi tertentu dan yang kedua, adanya kesempatan untuk memperkuat kolaborasi lintas klaster agar negara-negara *perifir* melalui proyek kolaboratif multinegara atau riset bersama antar negara.



Sumber : Karya Penulis sendiri, 2026

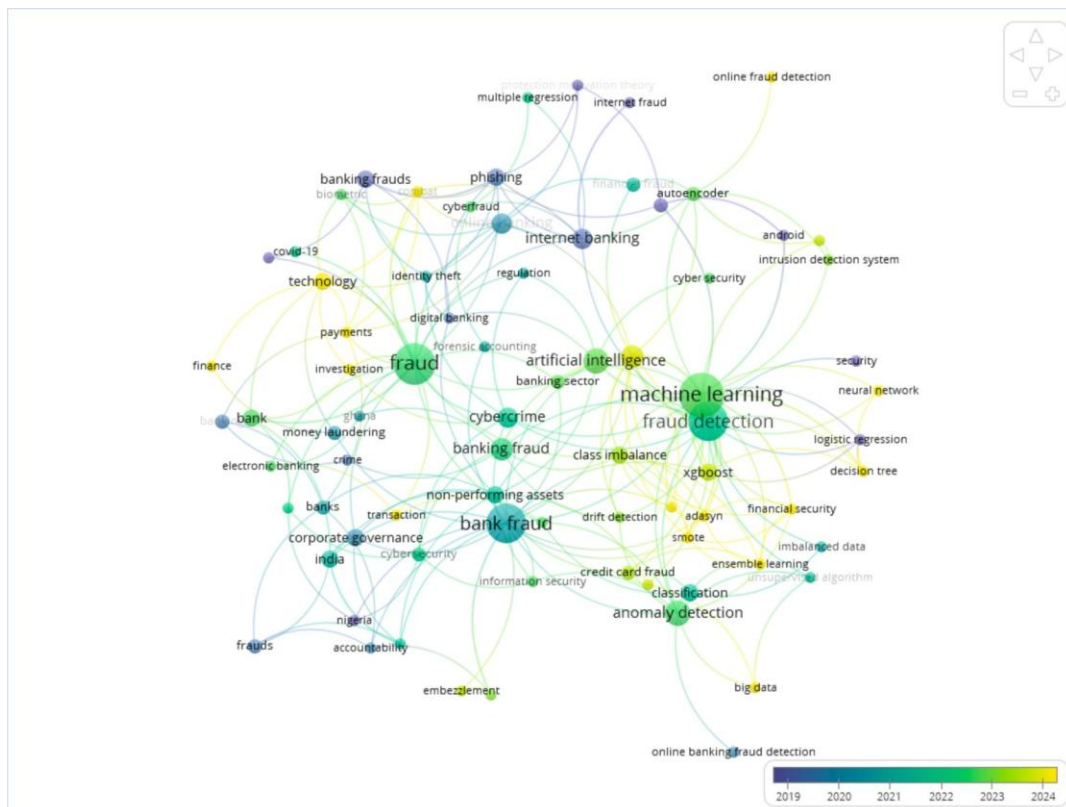
Gambar 5. Jaringan Kepenulisan bersama antar negara

Analisis Kata Kunci

Jaringan ko-kemunculan kata kunci (*keyword co-occurrence*) menggambarkan struktur tema riset dan keterkaitan kata kunci yang muncul dalam publikasi. *Node* yang lebih besar menunjukkan kata kunci yang sering muncul, sementara kedekatan dan kerapatan garis menunjukkan kata kunci yang sering muncul bersama dalam dokumen yang sama. Kata kunci utama yang dominan pada pusat jaringan yaitu *machine learning*, *fraud detection*, dan *bank fraud* atau *banking fraud*. Dominasi kata kunci tersebut menunjukkan bahwa literatur dalam topik ini fokus pada penerapan metode pembelajaran mesin untuk mendeteksi kecurangan, terutama pada lingkungan layanan keuangan dan perbankan.

Pada sekitar kata kunci utama tersebut, jaringan juga memperlihatkan beberapa kata kunci yang cukup besar. Pertama, keamanan siber dan ancaman digital seperti *cybercrime*, *phishing*, dan *intrusion detection system*, yang menunjukkan keterkaitan erat antara *fraud* dan aspek keamanan sistem. Kedua, ekosistem layanan keuangan digital seperti *internet banking* dan *digital banking* yang menunjukkan bahwa riset banyak berfokus pada *platform* transaksi digital yang rentan terhadap pola *fraud* yang canggih. Ketiga, pendekatan analitik atau metode seperti *anomaly detection*, *classification*, *ensemble learning*, dan algoritma tertentu, sehingga tampak berbagai teknik yang digunakan untuk meningkatkan akurasi deteksi. Pemetaan warna yang menunjukkan waktu publikasi (2019 – 2024) menunjukkan dinamika perkembangan riset bergerak dari pembahasan *fraud* secara umum ke pendekatan *data-driven*, memanfaatkan

AI/ML dan teknik deteksi adaptif untuk berbagai pola *fraud* yang terus berubah seiring perkembangan teknologi.



Sumber : Karya Penulis sendiri, 2026

Gambar 7. Jaringan ko-kemunculan kata kunci

Tabel berikut menyajikan temuan untuk (RQ4), yang menganalisis strategi, kebijakan dan teknologi yang direkomendasikan dalam literatur untuk mengurangi dan mencegah fraud di sektor perbankan. Tabel 2 ini merangkum pendekatan strategis yang dinilai efektif, termasuk penerapan sistem deteksi dini berbasis kecerdasan buatan, peningkatan pengawasan internal, pelatihan anti-fraud bagi staf bank, serta kolaborasi antara regulator, lembaga keuangan, dan penegak hukum. Selain itu, tabel ini juga mencerminkan kebijakan regulasi yang berkembang secara global dalam menghadapi modus kejahatan perbankan yang semakin kompleks. Temuan ini memberikan wawasan tentang praktik terbaik dan rekomendasi kebijakan yang dapat memperkuat integritas sistem keuangan serta melindungi nasabah dan lembaga perbankan dari risiko fraud.

Tabel 2. Strategi dan Kebijakan yang direkomendasikan dalam literatur untuk mengurangi dan mencegah fraud di sektor perbankan

No	Strategi/Kebijakan	Teknologi	Penelitian
1	Pengembangan model deteksi fraud berbasis machine learning dengan teknik optimasi seperti tuning parameter dan seleksi fitur.	ML: Random Forest, Decision Tree, SVM, Logistic Regression, Neural Network, Hyperparameter Tuning, GPU/FPGA	(Tariq et al. 2024), (Adesh et al. 2024), (Lestari et al. 2024).
2	Penanganan data tidak seimbang dan penguatan deteksi melalui metode pencarian dan klasifikasi canggih.	Adversarial Augmentation, Vortex Search Algorithm, 1DCNN	(Adesh et al. 2024), Reisig, Holtfreter, dan Cullen (2024)
3	Deteksi fraud real-time atau otomatis dalam layanan keuangan menggunakan pembelajaran tidak terawasi dan sistem berbasis AI	Unsupervised Learning, Ensemble Models, AI Automation	(Lestari et al. 2024), (D.N et al. 2024), (G. et al. 2024)

No	Strategi/Kebijakan	Teknologi	Penelitian
4	Identifikasi pola anomali transaksi menggunakan metode clustering dan algoritma seleksi fitur.	Louvain-coloring Clustering, HGRO Feature Selection, OC-LSTM	(Jeong, Lee, and Kim 2024), Balasankula et al. (2024)
5	Pencegahan akses tidak sah melalui deteksi intrusi jaringan yang cerdas dan berbasis big data.	XGBoost, Intelligent Network Intrusion Detection System (SDN)	(Akinbowale, Mashigo, and Zerihun 2024)
6	Peningkatan keamanan siber bank melalui pemanfaatan AI untuk pemantauan aktivitas dan serangan siber.	AI for Cybersecurity, Threat Monitoring, Fraud Intelligence	(Nobel et al. 2024), Singh et al. (2024)
7	Edukasi publik tentang risiko siber termasuk phishing, e-commerce fraud, dan perbankan digital.	Awareness Campaigns, Phishing Detection Tools	Vashistha dan Tiwari (2024)
8	Otentikasi dan verifikasi pengguna melalui agen cerdas dan deteksi biometrik tanda tangan/pemalsuan	Intelligent Authentication Agents, Tensorflow, Signature Geometry	(Kulmie and Ibrahim 2024), (Mardiansyah et al. 2024)
9	Verifikasi forensik pada dokumen fisik berbasis sensor dan jaringan saraf tiruan.	2D Lab Sensor, Artificial Neural Networks	(Teng et al., 2024)
10	Analisis kejahatan siber di tingkat nasional untuk menyusun strategi kebijakan nasional berbasis data besar.	National Cybercrime ML Analysis, Predictive Modelling	(Rao et al., 2024)
11	Pengembangan Sistem Pendukung Keputusan (DSS) dalam mengelola fraud di perbankan digital.	DSS (Decision Support Systems)	(Johora et al., 2024)
12	Evaluasi kerangka manajemen risiko untuk mengurangi kegagalan dalam pengendalian fraud.	Risk Management Models, Governance Frameworks	(Pinjarkar et al., 2024)
13	Pemanfaatan AI dalam mendeteksi operasi penipuan bank secara holistik.	Artificial Intelligence (AI)	(Lakshmi et al., 2024)
14	Studi kepribadian (Dark Triad) dalam hubungan dengan fraud dan tata kelola di sektor perbankan.	Behavioral & Governance Analysis	(Sinha, 2024)
15	Teknologi biometrik dan blockchain untuk melindungi transaksi perbankan dari kejahatan dunia maya.	Rain Drop Service, Biometric Verification, Weighted Fair Blockchain (WFB) Algorithm	(Naik, Jauhar, & Prasad, 2023)

Sumber : Karya penulis sendiri, 2025

Penelitian-penelitian terkini dalam sektor perbankan menunjukkan bahwa strategi deteksi dan pencegahan fraud harus berbasis pada integrasi teknologi canggih dan pendekatan kebijakan yang adaptif terhadap dinamika risiko siber. Salah satu temuan utama yang banyak diangkat dalam literatur adalah efektivitas machine learning (ML) dalam mendeteksi pola-pola anomali transaksi yang kompleks dan sulit dikenali secara manual. Berbagai algoritma seperti Random Forest, SVM, Neural Network, dan Decision Tree telah digunakan secara luas, terutama dalam kombinasi dengan teknik hyperparameter tuning dan pemrosesan paralel berbasis GPU/FPGA, guna meningkatkan akurasi dan efisiensi ((Tariq et al. 2024);(Adesh et al. 2024); (Lestari et al. 2024).

Masalah ketidakseimbangan data, yang kerap menjadi tantangan dalam pelatihan model, diatasi melalui teknik augmentation seperti Adversarial Augmentation dan algoritma pencarian seperti Vortex Search Algorithm, serta penggunaan model CNN satu dimensi (1DCNN) (Adesh et al. 2024). Untuk deteksi fraud secara real-time, pendekatan unsupervised learning dan sistem otomatis berbasis AI menjadi semakin relevan dalam konteks layanan keuangan digital (Lestari et al. 2024).

Literatur juga menggarisbawahi pentingnya clustering dan seleksi fitur dalam mengidentifikasi anomali, sebagaimana terlihat pada penggunaan metode seperti Louvain-coloring clustering, HGRO, dan OC-LSTM ((Jeong et al. 2024) Balasankula et al. (2024)). Sementara itu, peningkatan keamanan jaringan dan pencegahan akses tidak sah dilakukan

melalui integrasi sistem deteksi intrusi berbasis big data dan algoritma seperti XGBoost serta pendekatan berbasis Software Defined Network (SDN) (Akinbowale et al. 2024).

Pendekatan berbasis AI juga digunakan untuk threat monitoring dan intelijen fraud guna merespons serangan siber secara proaktif ((Nobel et al. 2024), Singh et al. (2024). Di sisi lain, penguatan edukasi publik terhadap risiko siber seperti phishing dan penipuan e-commerce juga menjadi strategi penting yang didukung oleh teknologi seperti phishing detection tools (Vashistha dan Tiwari, 2024). Inovasi lain mencakup penggunaan agen autentikasi cerdas dan teknologi biometrik seperti TensorFlow serta deteksi tanda tangan palsu, yang terbukti meningkatkan akurasi verifikasi pengguna (Kulmie and Ibrahim 2024); (Mardiansyah et al. 2024).

Pendekatan forensik juga turut dikembangkan melalui integrasi sensor laboratorium 2D dan jaringan saraf tiruan, khususnya dalam memverifikasi keaslian dokumen fisik (Teng et al., 2024). Untuk kepentingan kebijakan makro, analisis kejahatan siber di tingkat nasional dilakukan dengan pendekatan berbasis predictive modelling yang mengandalkan data besar (Rao et al., 2024). Sistem pendukung keputusan (Decision Support Systems) juga dikembangkan sebagai bagian dari sistem manajemen fraud digital (Johora et al., 2024).

Literatur lain menekankan pentingnya evaluasi kerangka manajemen risiko untuk meminimalisasi kegagalan pengendalian (Pinjarkar et al., 2024), serta penggunaan AI dalam deteksi penipuan secara menyeluruh (Lakshmi et al., 2024). Pendekatan berbasis kepribadian juga dikaji, termasuk studi terkait Dark Triad untuk memahami kecenderungan fraud di sektor perbankan (Sinha, 2024). Akhirnya, integrasi teknologi biometrik dan blockchain melalui pendekatan seperti Rain Drop Service dan Weighted Fair Blockchain (WFB) Algorithm telah menunjukkan potensi signifikan dalam memperkuat keamanan transaksi dan menurunkan risiko penipuan (Naik, Jauhar, & Prasad, 2023).

KESIMPULAN

Penelitian ini berhasil memetakan dinamika dan tren global dalam kajian penipuan di sektor perbankan melalui pendekatan bibliometrik terhadap puluhan artikel ilmiah terindeks. Hasil analisis menunjukkan bahwa sejak tahun 2019 terjadi lonjakan signifikan dalam publikasi ilmiah terkait, yang dipicu oleh meningkatnya digitalisasi sistem keuangan dan kompleksitas modus kejahatan siber. Tema dominan meliputi penggunaan algoritma machine learning untuk deteksi fraud, pemanfaatan blockchain dalam keamanan transaksi, serta penerapan sistem berbasis IoT dan big data analytics. Selain itu, penelitian juga memperlihatkan keterlibatan multidisiplin termasuk ilmu komputer, keuangan, dan hukum dalam menjawab tantangan keamanan perbankan modern. Negara berkembang turut aktif berkontribusi, menandakan urgensi perlindungan sistem keuangan di tengah peningkatan inklusi digital.

Implikasi

Secara teoritis, temuan ini memperkuat kebutuhan integrasi antara ilmu teknologi dan keuangan dalam membentuk sistem pendeteksian fraud yang adaptif dan cerdas. Bagi praktisi perbankan, studi ini menggarisbawahi pentingnya investasi dalam teknologi prediktif seperti AI dan blockchain untuk mengurangi risiko kerugian akibat kejahatan finansial. Sementara itu, bagi pembuat kebijakan, diperlukan regulasi yang responsif terhadap dinamika modus kejahatan siber, termasuk kebijakan perlindungan data dan standar keamanan digital. Dari sisi sosial, peningkatan literasi digital bagi nasabah juga menjadi bagian penting dari strategi mitigasi fraud, terutama di wilayah yang mengalami percepatan adopsi layanan perbankan digital pasca pandemi.

Keterbatasan dan Penelitian Masa Depan

Meskipun memberikan kontribusi yang berarti dalam memahami lanskap penelitian global tentang penipuan di sektor perbankan, studi ini memiliki beberapa keterbatasan.

Pertama, cakupan literatur yang dianalisis masih didominasi oleh publikasi dari negara maju, sehingga potensi variasi modus dan respons terhadap fraud di negara berkembang belum tergambarkan secara utuh. Kedua, mayoritas penelitian menggunakan pendekatan kuantitatif dan teknik komputasional, yang cenderung mengabaikan dimensi sosial, psikologis, dan budaya dari pelaku maupun korban penipuan. Ketiga, keterbatasan basis data dan rentang waktu analisis berisiko melewatkan dinamika jangka panjang serta artikel penting yang diterbitkan di luar platform Scopus.

Ke depan, penelitian perlu memperluas cakupan dan kedalaman analisis dengan berbagai strategi. Pertama, studi kualitatif dapat dilakukan untuk menggali narasi korban, pelaku, serta respons institusi keuangan secara lebih mendalam. Kedua, pendekatan lintas disiplin, misalnya menggabungkan studi kriminologi, psikologi, dan ekonomi perilaku akan memberikan pemahaman yang lebih holistik terhadap motivasi dan mekanisme terjadinya fraud. Ketiga, pengembangan studi longitudinal diperlukan untuk mengamati efektivitas sistem deteksi dan pencegahan fraud dalam jangka waktu yang lebih panjang. Keempat, kajian perbandingan antarnegara atau antarwilayah dapat mengungkap best practices dalam pengelolaan risiko fraud yang kontekstual dan berbasis teknologi. Dengan demikian, penelitian masa depan diharapkan tidak hanya memperluas cakrawala keilmuan, tetapi juga berkontribusi pada perumusan kebijakan keamanan finansial yang inklusif dan adaptif.

REFERENSI

- AbouGrad, H., & Sankuru, L. (2025). Online Banking Fraud Detection Model: Decentralized Machine Learning Framework to Enhance Effectiveness and Compliance with Data Privacy Regulations. *Mathematics*, 13(13), 1–19. <https://doi.org/10.3390/math13132110>
- Adesh, A., G, S., Shetty, J., & Xu, L. (2024). Local outlier factor for anomaly detection in HPC systems. *Journal of Parallel and Distributed Computing*, 192(April), 104923. <https://doi.org/10.1016/j.jpdc.2024.104923>
- Al-Hashedi, K. G., & Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. *Computer Science Review*, 40. <https://doi.org/10.1016/j.cosrev.2021.100402>
- Alzahrani, A. O., & Alenazi, M. J. F. (2021). Designing a network intrusion detection system based on machine learning for software defined networks. *Future Internet*, 13(5). <https://doi.org/10.3390/fi13050111>
- Akinbowale, O. E., Mashigo, P., & Zerihun, M. F. (2024). Analysis of cyberfraud in the South African banking industry: a multiple regression approach. *Journal of Financial Crime*, 31(4), 952–973. <https://doi.org/10.1108/JFC-04-2023-0094>
- Byrapu Reddy, S. R., Kanagala, P., Ravichandran, P., Pulimamidi, D. R., Sivarambabu, P. V., & Polireddi, N. S. A. (2024). Effective fraud detection in e-commerce: Leveraging machine learning and big data analytics. *Measurement: Sensors*, 33(December 2023), 101138. <https://doi.org/10.1016/j.measen.2024.101138>
- Carminati, M., Caron, R., Maggi, F., Epifani, I., & Zanero, S. (2015). BankSealer: A decision support system for online banking fraud analysis and investigation. *Computers and Security*, 53, 175–186. <https://doi.org/10.1016/j.cose.2015.04.002>
- Cirqueira, D., Nedbal, D., Helfert, M., & Bezbradica, M. (2020). Scenario-Based Requirements Elicitation for User-Centric Explainable AI: A Case in Fraud Detection. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 12279 LNCS*. Springer International Publishing. https://doi.org/10.1007/978-3-030-57321-8_18
- Chen, Y., Zhao, C., Xu, Y., Nie, C., & Zhang, Y. (2025). Deep Learning in Financial Fraud Detection: Innovations, Challenges, and Applications. *Data Science and Management*. <https://doi.org/10.1016/j.dsm.2025.08.002>

- D.N, N., C.C., O., C.I, A., K.C, O., & Richard-Nnabu, N. (2024). *Intelligent Authentication Agent Model for Detection of ATM Card Fraud in Nigeria* (pp. 1541–1547). Grenze Scientific Society.
- Firdaus, A., Anuar, N. B., Karim, A., & Razak, M. F. A. (2018). Discovering optimal features using static analysis and a genetic search based method for Android malware detection. *Frontiers of Information Technology & Electronic Engineering*, 19(6), 712–736. <https://doi.org/10.1631/FITEE.1601491>
- Hassan, N. C., Abdul-Rahman, A., Hamid, S. N. A., & Amin, S. I. M. (2024). What factors affecting investment decision? The moderating role of fintech self-efficacy. *PLoS ONE*, 19(4 April), 1–25. <https://doi.org/10.1371/journal.pone.0299004>
- H. Teng, C. Wang, Q. Yang, X. Chen and R. Li, "Leveraging Adversarial Augmentation on Imbalance Data for Online Trading Fraud Detection," in *IEEE Transactions on Computational Social Systems*, vol. 11, no. 2, pp. 1602-1614, April 2024, <https://doi.org/10.1109/TCSS.2023.3240968>
- G., M. R., G., A., G., G., P., K., & R., S. (2024). *Online Fraudulence Detection Based on Decision Support System in Digital Banking*. Auricle Global Society of Education and Research.
- Gepp, A., Linnenluecke, M. K., O'Neill, T. J., & Smith, T. (2018). Big data techniques in auditing research and practice: Current trends and future opportunities. *Journal of Accounting Literature*, 40(February), 102–115. <https://doi.org/10.1016/j.acclit.2017.05.003>
- Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, 10(1), 79–91. <https://doi.org/10.5281/zenodo.58523>
- Jeong, C. W., Lee, Y. J., & Kim, H. J. (2024). Analysis of Periodic Marks for Forensic Document Examination using Boosting Algorithms. *Palpu Chongi Gisul/Journal of Korea Technical Association of the Pulp and Paper Industry*, 56(4), 65–73. <https://doi.org/10.7584/JKTAPPI.2024.8.56.4.65>
- Johora, F. T., Hasan, R., Farabi, S. F., Alam, M. Z., Sarkar, I., & Mahmud, A. A. (2024). *AI advances: Enhancing banking security with fraud detection*. In Proceedings of the 2024 First International Conference on Technological Innovations and Advance Computing (TIACOMP) (pp. 289–294). IEEE. <https://doi.org/10.1109/TIACOMP64125.2024.00055>
- Kannagi, A., Gori Mohammed, J., Sabari Giri Murugan, S., & Varsha, M. (2021). Intelligent mechanical systems and its applications on online fraud detection analysis using pattern recognition K-nearest neighbor algorithm for cloud security applications. *Materials Today: Proceedings*, 81(2), 745–749. <https://doi.org/10.1016/j.matpr.2021.04.228>
- Khan, T. A., Tulsi, J., Alam, M., Kadir, K., Ali, K. M., & Mazliham, M. S. (2025). Analysis and visualization of fraud detection patterns through data mining and classification using MLP and hybrid deep learning model. *Egyptian Informatics Journal*, 32(November), 100829. <https://doi.org/10.1016/j.eij.2025.100829>
- Kulmie, D. A., & Ibrahim, M. S. (2024). Bank Corporate Governance: Shield against Fraud. *Journal of Ecohumanism*, 3(3), 1917–1932. <https://doi.org/10.62754/joe.v3i3.3582>
- Lakshmi, A. A., Reddy, G. S., Reddy, M. S., & Kathirisetty, N. (2024). *Offline signature forgery detection based on geometric measures using TensorFlow model*. In Proceedings of the 2024 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC) (pp. 1–7). IEEE. <https://doi.org/10.1109/ASSIC60049.2024.10507928>
- Lestari, S., Adawiyah, W. R., Alhamidi, A. L., Prayogi, J., & Haryanto, R. (2024). Navigating perilous seas: unmasking online banking frauds, perceived usefulness, fear of

- cybercrime and distrust in online banking. *Safer Communities*, 23(4), 444–464. <https://doi.org/10.1108/SC-04-2024-0018>
- Logeswari, G., Bose, S., & Anitha, T. (2023). An Intrusion Detection System for SDN Using Machine Learning. *Intelligent Automation and Soft Computing*, 35(1), 867–880. <https://doi.org/10.32604/iasc.2023.026769>
- Mardiansyah, H., Suwilo, S., Nababan, E. B., & Efendi, S. (2024). The role of Louvain-coloring clustering in the detection of fraud transactions. *International Journal of Electrical and Computer Engineering*, 14(1), 608–616. <https://doi.org/10.11591/ijece.v14i1.pp608-616>
- Moro, S., Cortez, P., & Rita, P. (2015). Business intelligence in banking: A literature analysis from 2002 to 2013 using text mining and latent Dirichlet allocation. *Expert Systems with Applications*, 42(3), 1314–1324. <https://doi.org/10.1016/j.eswa.2015.09.024>
- Ming, R., Abdelrahman, O., Innab, N., & Ibrahim, M. H. K. (2024). Enhancing fraud detection in auto insurance and credit card transactions: a novel approach integrating CNNs and machine learning algorithms. *PeerJ Computer Science*, 10, 1–35. <https://doi.org/10.7717/peerj-cs.2088>
- Naik, S. P., Jauhar, D. A., & Prasad, C. V. V. S. N. (2023). *Value relevance of enterprise risk management: the Indian case*. *International Journal of Business Continuity and Risk Management*, 13(3), 229–247. <https://doi.org/10.1504/IJBCRM.2023.132904>
- Nana Kwame Gyamfi, D. J.-D. A. (2018). Bank Fraud Detection Using Support Vector Machine. *2018 IEEE 9th Annual Information Technology Electronics and Mobile Communication Conference Iemcon 2018*, Pp. 37–41, 8614994, 37–41.
- Nobel, S. M. N., Sultana, S., Singha, S. P., Chaki, S., Mahi, M. J. N., Jan, T., Barros, A., & Whaiduzzaman, M. (2024). Unmasking Banking Fraud: Unleashing the Power of Machine Learning and Explainable AI (XAI) on Imbalanced Data. *Information (Switzerland)*, 15(6), 1–22. <https://doi.org/10.3390/info15060298>
- Odufisan, O. I., Abbulimen, O. V., & Ogunti, E. O. (2025). Harnessing artificial intelligence and machine learning for fraud detection and prevention in Nigeria. *Journal of Economic Criminology*, 7(January), 100127. <https://doi.org/10.1016/j.jecon.2025.100127>
- Owusu, A. (2025). Achieving operational excellence through artificial intelligence: The case of Ghanaian banks. *International Journal of Information Management Data Insights*, 5(2). <https://doi.org/10.1016/j.jjime.2025.100377>
- Pinjarkar, L., Hete, P. R., Mattada, M., Nejakar, S., Agrawal, P., & Kaur, G. (2024). *An examination of prevalent online scams: Phishing attacks, banking frauds, and e-commerce deceptions*. In *Proceedings of the 2024 Second International Conference on Advances in Information Technology (ICAIT)* (pp. 1–6). IEEE. <https://doi.org/10.1109/ICAIT61638.2024.10690377>
- Rao, G. B. N., Kumar, A., Kumar, N., & Raj, P. (2024). *Efficient intelligent network intrusion detection for SDN using XGBoost*. In *Proceedings of the 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1–9). IEEE. <https://doi.org/10.1109/ICCCNT61001.2024.10723841>
- Ramos, S., Perez-Lopez, J. A., Abreu, R., & Nunes, S. (2024). Impact of fraud in Europe: Causes and effects. *Heliyon*, 10(22), e40049. <https://doi.org/10.1016/j.heliyon.2024.e40049>
- Reisig, M.D., Holtfreter, K. & Cullen, F.T. Faith in Trump and the willingness to punish white-collar crime: Chinese Americans as an out-group. *J Exp Criminol* 20, 123–149 (2024). <https://doi.org/10.1007/s11292-022-09528-8>
- Singh, K.J., Kapoor, D.S., Singh, K.R., Kalucha, C., Alagh, G., Thakur, K. and Sharma, A. (2024). Comparative Evaluation of Machine Learning Algorithms for Bank Fraud Detection. In *Integrating Metaheuristics in Computer Vision for Real-World*

- Optimization Problems (eds S. Mahajan, K. Joshi, A.K. Pandit and N. Pathak). <https://doi.org/10.1002/9781394230952.ch4>
- Sinha, A. (2024). Fraud Risk Management in Banks: An Overview of Failures and Best Practices. In I. Management Association (Ed.), *Research Anthology on Business Law, Policy, and Social Responsibility* (pp. 829-847). IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3693-2045-7.ch044>
- Sood, P., & Bhushan, P. (2020). A structured review and theme analysis of financial frauds in the banking industry. *Asian Journal of Business Ethics*, 9(2), 305–321. <https://doi.org/10.1007/s13520-020-00111-w>
- Swati Gupta. (2025). Hacking the System: A Deep Dive into the World of E-Banking Crime. In *The Techno-Legal Dynamics of Cyber Crimes in Industry 5.0*. <https://doi.org/10.1002/9781394242177.ch7>
- Sharma, N., Sharma, D., & Aggarwal, A. (2020). Emerging trends and growth of banking frauds in India: a substantial obstacle in the pathway of sustainable development. *World Review of Science, Technology and Sustainable Development*, 16(3), 257–274. <https://doi.org/10.1504/WRSTSD.2020.113060>
- Shakil, K. A., Zareen, F. J., Alam, M., & Jabin, S. (2020). BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud. *Journal of King Saud University - Computer and Information Sciences*, 32(1), 57–64. <https://doi.org/10.1016/j.jksuci.2017.07.001>
- Singh, J., Singh, G., Gahlawat, M., & Prabha, C. (2022). Big Data as a Service and Application for Indian Banking Sector. *Procedia Computer Science*, 215, 878–887. <https://doi.org/10.1016/j.procs.2022.12.090>
- Tariq, E., Akour, I., Al-Shanableh, N., Alquqa, E. K., Alzboun, N., Al-Hawary, S. I. S., & Alshurideh, M. T. (2024). How cybersecurity influences fraud prevention: An empirical study on Jordanian commercial banks. *International Journal of Data and Network Science*, 8(1), 69–76. <https://doi.org/10.5267/j.ijdns.2023.10.016>
- U. R. Balasankula, B. Poojitha, S. Chekurtha, K. Buyya, H. Bala and P. R. V, "Banking Fraud Detection Using Machine Learning Algorithms," 2024 5th International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2024, pp. 1228-1233, <https://doi.org/10.1109/ICESC60852.2024.10689731>
- Vanini, P., Rossi, S., Zvizdic, E., & Domenig, T. (2023). Online payment fraud: from anomaly detection to risk management. *Financial Innovation*, 9(1). <https://doi.org/10.1186/s40854-023-00470-w>
- Vashistha, A., Tiwari, A.K. Building Resilience in Banking Against Fraud with Hyper Ensemble Machine Learning and Anomaly Detection Strategies. *SN COMPUT. SCI.* 5, 556 (2024). <https://doi.org/10.1007/s42979-024-02854-w>