Website:
ejournal.umm.ac.id/index.php/jrak

***Correspondence:**
tarjo@trunojoyo.ac.id

DOI: 10.22219/jrak.v13i3.28487

Citation:
Mahya, L., Tarjo., Sanusi, Z, M., Kurniawan, F, A. (2023). Intelligent Automation Of Fraud Detection And Investigation:A Bibliometric Analysis Approach. Jurnal Reviu Akuntansi Dan Keuangan, 13(3), 588-613.

Article Process
Submitted:
August 8, 2023

Reviewed:
August 14, 2023

Revised:
October 12, 2023

Accepted:
October 12, 2023

Published:
October 12, 2023

Office:
Department of AccountingUniversity of Muhammadiyah Malang
GKB 2 Floor 3.
Jalan Raya Tlogomas 246, Malang, East Java, Indonesia

P-ISSN: 2615-2223
E-ISSN: 2088-0685

Article Type: Research Paper

INTELLIGENT AUTOMATION OF FRAUD DETECTION AND INVESTIGATION:A BIBLIOMETRIC ANALYSIS APPROACH

Lummatul Mahya[1], Tarjo[2*], Zuraidah Mohd Sanusi[3], Fitri Ahmad Kurniawan

Affiliation:

[1,2,4]Fakultas Ekonomi dan Bisnis, Universitas Trunojoyo Madura, Indonesia

[3]Accounting Research Institute, Universiti Teknologi MARA, Shah Alam, Malaysia

ABSTRACT

Purpose:*This study aims to examine the use of intelligent automation in the process of detecting and investigating fraud.*

Methodology/approach:*This research is a bibliometric-based systematic literature review (SLR) related to fraud detection. The research sample consisted of 75 articles obtained from the Science Direct, Emerald Insight, IEE, and MDPI databases for the period 2020–2023.*

Findings: *The results of the research show that machine learning and deep learning are the most popular fraud detection techniques used by researchers, and the field of credit card fraud is the most popular field used as a research object. The fields of property insurance, health, cyber phishing, taxation, Shell companies, social programs, Ponzi schemes, and supply chain management are the ones that have the least amount of research, namely only one article for each of these fields.*

Practical implications: *The result show that there are smart tools in detecting fraud in several fields, but it has not been explained whether the existence of these tools can reduce fraud.*

Originality/value: *This research provides novelty in the use of intelligent automation in the process of detecting and investigating fraud.*

***KEYWORDS**: Bibliometrics; Fraud Detection; Systematic Literature Review (SLR).*

ABSTRAK

Tujuan penelitian: Penelitian ini bertujuan untuk meneliti penggunaan otomatisasi cerdas dalam proses deteksi dan investigasi tindakan *fraud.*

Metode/Pendekatan: Penelitian ini merupakan *Systematic Literature Review*(SLR) berbasis bibliometrik terkait deteksi *fraud*. Sampel penelitian tediri dari 75 artikel yang diperoleh dari *database* Science Direct, Emerald Insight, IEE, dan MDPI dengan periode 2020-2023.

Hasil: Hasil penelitian menunjukkan bahwa *machine learning* dan *deep learning* merupakan teknik deteksi *fraud* paling populer yang digunakan oleh peneliti, kemudian bidang *credit card fraud* merupakan bidang yang paling populer yang dijadikan objek penelitian. Bidang Asuransi Properti, kesehatan, *cyber phising*, Perpajakan, *Shell Company*, Program Sosial, skema Ponzi dan *Supply chain* merupakan bidang yang memiliki jumlah penelitian paling sedikit yakni hanya satu artikel untuk masing-masing bidang tersebut.

Implikasi praktik: Temuan menunjukkan bahwa terdapat alat cerdas dalam mendeteksi tindakan *fraud* di beberapa bidang, akan tetapi belum dijelaskan apakah dengan adanya alat tersebut mampu mengurangi tindakan *fraud.*

Orisinalitas/kebaharuan: Penelitian ini memberikan kebaruan dalam penggunaan otomatisasi cerdas dalam proses deteksi dan investigasi tindakan *fraud*.

KATA KUNCI: Bibliometrik; Deteksi Fraud; *Systematic Literature Review (SLR).*

PENDAHULUAN

Fraud merupakan masalah global yang memengaruhi organisasi di setiap wilayah dan industri di seluruh dunia. Mengukur luas sebenarnya dari kerusakan yang disebabkan oleh *fraud* merupakan pekerjaan yang menantang karena sifat penyembunyian dan *fraud* yang melekat di sebagian besar skema. Berdasarkan survei yang diselidiki dari januari 2020 hingga januari 2021 terdapat kasus *fraud* sebanyak 2.110 kasus yang tersebar di 133 negara dengan perkiraan kerugian mencapai $3,6 Miliar, dengan rata-rata nilai kerugian perkasus sebesar $1.783.000,00. Skema *fraud* tertinggi terletak pada kasus penyalahgunaan aset sebesar 86%, kemudian korupsi sebesar 50%, dan *fraud* laporan keuangan sebesar 9% (ACFE, 2022).

Munculnya penggunaan teknologi modern tidak hanya menguntungkan masyarakat tetapi juga menarik para penipu dan penjahat menyalahgunakan teknologi untuk keuntungan finansial. Penipuan melalui internet telah meningkat secara dramatis, mengakibatkan kerugian miliaran dolar bagi pelanggan dan penyedia layanan seluruh dunia (Ali et al., 2019). Situasi lain yang ditimbulkan oleh meningkatnya digitalisasi adalah berkembangnya produk dan layanan keuangan baru yang membuat metode deteksi yang ada sulit untuk beradaptasi (Zhu et al., 2021). Deteksi *fraud* merupakan langkah penting dalam proses penyelidikan penipuan karena kecepatan dan cara deteksi penipuan dapat berdampak besar terhadap besarnya penipuan yang terjadi. Hal teresebut juga merupakan komponen penting dari pencegahan penipuan, karena pemeriksa penipuan dapat mengambil langkah-langkah untuk meningkatkan cara mereka mendeteksi penipuan di dalam organisasi (ACFE, 2022).

Penggunaan teknologi informasi dan komunikasi dalam menjalakan bisnis harus disertai dengan pengembangan konsep otorisasi. Ketika auditor ditugaskan untuk memeriksa semua transaksi, sedangkan data sudah ada dalam bentuk digital, maka diperlukan proses berbasis komputer untuk menganalisisnya. Proses tersebut memungkinkan auditor untuk melakukan pemeriksaan ekstensif dalam jangka waktu yang dapat diterima dan dengan usaha yang wajar. Setelah algoritma ditentukan, hanya dibutuhkan model komputasi untuk mengevaluasi jumlah data yang lebih besar. Kontribusi ini menyajikan proses analisis data berbasis Teknologi Informasi (TI) yang dapat digunakan untuk mengidentifikasi kegiatan penipuan (*fraud*)(Flegel et al., 2010).

Artificial intelligence (AI) merupakan bagian dari Teknologi Informasi yang menggunakan sistem komputer dalam proses kerjanya. *Robotic process automation* atau *intelligent automation* merupakan (kombinasi *Artificial intelligence* dan *automation*) mulai mengubah cara bisnis, hal ini dilakukan di hampir setiap sektor perekonomian.*Intelligent automation systems* mendeteksi dan memproduksi sejumlah besar informasi dan dapat diotomatisasi atas seluruh proses atau alur kerja, pembelajaran dan adaptasi saat data tersebut tidak ada (Patrick Laurent, 2015).

Metode deteksi penipuan tradisional, termasuk manual deteksi, tidak hanya mahal, tidak tepat, dan menghabiskan waktu, tapi juga tidak praktis. Kegiatan tersebut dilakukan untuk meminimalkan kerugian akibat tindakan penipuan, tetapi metode tersebut tidak terlalu efektif. *Artificial intelligence*, khususnya teknologi *machine learning*, menjadi salah satu metode terbesar dalam penemuan penipuan. *Data Mining* berkontribusi untuk mengidentifikasi penipuan dan bertindak cepat untuk menurunkan *overhead*. Jutaan dokumen dapat dicari melalui teknik *data mining* untuk menemukan pola dan mengidentifikasi tindakan penipuan (Ashtiani & Raahemi, 2022).

Metode untuk deteksi penipuan mengalami perkembangan pesat dalam beberapa dekade terakhir. Khususnya di era pasca pandemi, karena motif yang semakin intensif, bentuk yang berbahaya, dan skema penipuan keuangan yang semakin sulit untuk diidentifikasi secara akurat dan efisien. Oleh karena itu, para peneliti cenderung menggali informasi dari berbagai aspek untuk pemantauan yang komprehensif (Zhu et al., 2021). Penelitian (Pourhabibi et al., 2020) mengembangkan kerangka kerja untuk mensintesis literatur yang ada tentang penerapan metode *graph-based anomaly detection* dalam deteksi penipuan yang diterbitkan antara tahun 2007 dan 2018. Penelitian tersebut hanya berfokus pada artikel-artikel yang mengembangkan metode *graph-based anomaly detection*dalam proses deteksi penipuan. Penelitian (Cherif et al., 2023) menyajikan ulasan mendalam tentang penelitian mutakhir dalam mendeteksi dan memprediksi transaksi kartu kredit palsu yang dilakukan

dari tahun 2015 hingga 2021. Topik hanya berfokus pada bidang deteksi *fraud* kartu kredit dan teknologi yang digunakan dalam proses deteksi.

Beberapa peneliti juga melakukan penelitian terkait deteksi penipuan di beberapa bidang dengan teknik yang beragam, seperti penelitian (Vanhoeyveld et al., 2020) menggunakan teknik *anomaly detection* untuk deteksi *fraud* di bidang perpajakan. Kemudian (Dumitrescu et al., 2022) menggunakan *anomaly detection* untuk deteksi transaksi bank terkait *money laundering*.Penelitian (Chen et al., 2022) menggunakan model *hybrid credit scoring*dalam mendeteksi *fraud* bidang kredit, sedangkan (Bagga et al., 2020) menggunakan *en-semble learning* dalam deteksi *fraud* kartu kredit dan (Esenogho et al., 2022) menggunakan *neural network* dalam mendeteksi *fraud* kartu kredit.

Keberagaman topik di atas menunjukkan bahwa penelitian terkait deteksi dan investigasi *fraud*masih bisa dieksplor dan dianalisis lebih jauh lagi. Oleh sebab itu, penelitian ini akan menggabungkan seluruh penelitian terkait deteksi dan investigasi *fraud*. Hal tersebut didasari karena sebaran penelitian terkait deteksi dan investigas *fraud*sangat beragam dan belum dipetakan dengan baik sehingga perkembangannya tidak diketahui dengan jelas. Penelitian iniakan melakukan pemetaan terhadap topik yang berkaitan dengan deteksi dan investigasi *fraud*, seperti teknik-teknik yang digunakan oleh para peneliti dalam proses deteksi dan investigasi *fraud*. Kemudian pemetaan atas objek atau bidang yang diteliti, tren publikasi serta metode yang digunakan oleh para peneliti dalam melakukan penelitian.Metode ini memungkinkan untuk membongkar nuansa evolusioner dari bidang tertentu,dan menjelaskan hal-hal baru yang muncul di bidang tersebut.

Selanjutnya penelitian ini akan membahas terkait metodologi penelitian di bagian 2, termasuk kriteria pencarian dan seleksi data. Bagian 3 akan membahas terkait temuan dan pembahasan, kemudian kesimpulan dibahas di bagian 4.

METODE

Penelitian ini menggunakan pendekatan *SystematicLiterature Review*(SLR) bibliometrik yang bertujuan untuk mengidentifikasi model deteksi *fraud* kemudian melakukan pemetaan atas penelitian-penelitian tersebut. Pemetaan dalam penelitian ini terdiri dari, (1) Jenis penelitian yang dilakukan per tahun, (2) Publikasi, (3) Objek Penelitian (4) Jenis Deteksi yang digunakan. Penelitian ini juga menggunakan *software* VOSviewer dalam proses analis data. Sumber data berasal dari jurnal yang diterbitkan di Science Direct, Emerald Insight, IEE, MDPI dan Wiley. Penggunaan database tersebut didasarkan pada reputasi dan indeks yang dimiliki sangat bagus. Periode waktu yang digunakan dari tahun 2020 hingga tahun 2023 untuk melihat bagaimana kebaruan penelitian terkait penggunaan teknologidalam deteksi dan investigasi *fraud* saat masa pandemi COVID-19. Penelitian (Takefuji, 2023) melaporkan studi kasus mengenai penipuan ekonomi di Jepang, Amerika Serikat, Uni Eropa, Inggris, dan Moldova saat pandemi COVID-19 serta digitalisasi, tata kelola digital, *artificial intelligence* (AI) dapat mengurangi kasus-kasus penipuan tersebut.Kata kunci dalam mesin pencari adalah "Intelligent Automation Of Fraud Detection" dan "Fraud Detection".

Teknik *purposive sampling* dilakukan dalam pemilihan sampel. Artikel dipilih sesuai dengan tema penelitian yakni terkait "Intelligent Automation Of Fraud Detection" dengan periode 2020-2023.

Hasil database Science Direct sebanyak 788, Emerald Insight sebanyak 102, IEE sebanyak 86, MDPI sebanyak 217 dan Wiley sebanyak 521. Hasil penambangan data dengan kata kunci "Fraud Detection" menghasilkan artikel yang membahas semua tentang "fraud" dan "detection". Oleh sebab itu, dilakukan pemilihan beberapa kriteria artikel yang digunakan dalam penelitian ini. Artikel-artikel yang dijadikan sampel adalah (1) artikel yang berfokus membahas terkait deteksi atau investigasi*fraud* (2) artikel yang membahas deteksi *fraud* menggunakan teknologi informasi. Berdasarkan kriteria-kriteria tersebut jumlah sampel penelitian ini sebanyak 75 artikel.

HASIL DAN PEMBAHASAN

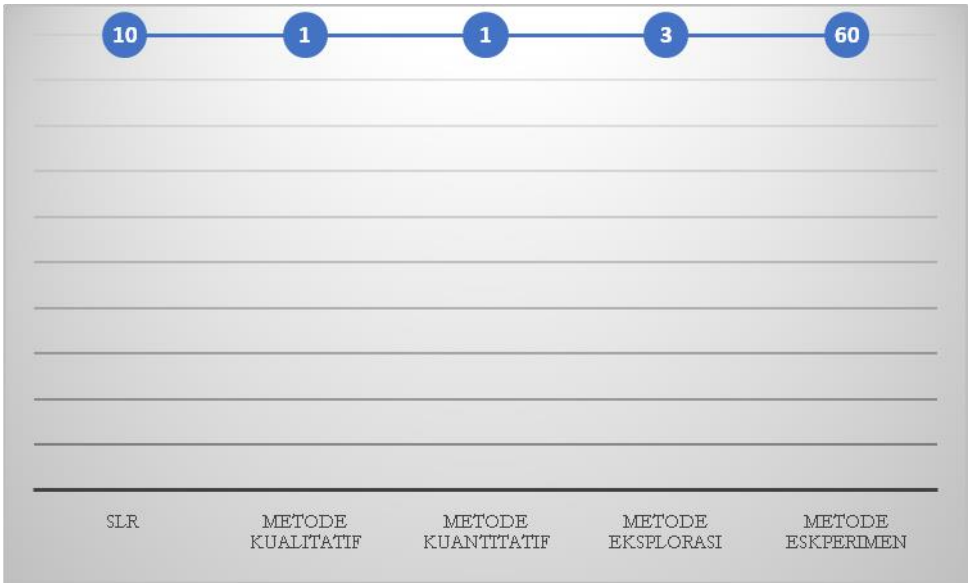
Jumlah sampel setelah melewati proses seleksi dengan *purposive sampling*berjumlah sebanyak 75 artikel. Berdasarkan gambar 1 jumlah artikel dari Science Direct (SD) sebanyak 38artikel, Emerald Insight (EI) sebanyak 04 artikel, IEE sebanyak 28 artikel, MDPI sebanyak 02 artikel, dan Wiley sebanyak 03 artikel.

Metode penelitian yang paling banyak dilakukan adalah penelitian dengan metode eksperimen sebanyak 60 artikel. Sedangkan jenis penelitian SLR (*SystematicLiterature Review)* sebanyak 10 artiel, Metode eksplorasi sebanyak 03 artikel, dan metode kuantitatif dan kualitatif masing-masing 01 artikel sebagaimana dijelaskan di gambar 1. Penelitian dengan metode eksperimen paling banyak dilakukan karena sebagian besar penelitian berfokus pada pengujian atas teknik atau model *intelligent automation* dalam deteksi penipuan.

Jumlah perilisan publikasi dari tahun 2020 hingga 2023 cukup fluktuatif. Tahun 2020 terdapat 23 publikasi terkait teknik atau model *intelligent automation* dalam melakukan deteksi penipuan, tahun 2021 sebanyak 23 artikel, 2022 sebanyak 27 artikel, dan paling rendah tahun 2023 sebanyak 2 artikel. Faktor yang mempengaruhi jumlah publikasi di tahun 2023 hanya sebanyak 2 artikel karena tahun tersebut merupakan awal tahun 2023 sehingga jumlah publikasi artikel masih rendah.

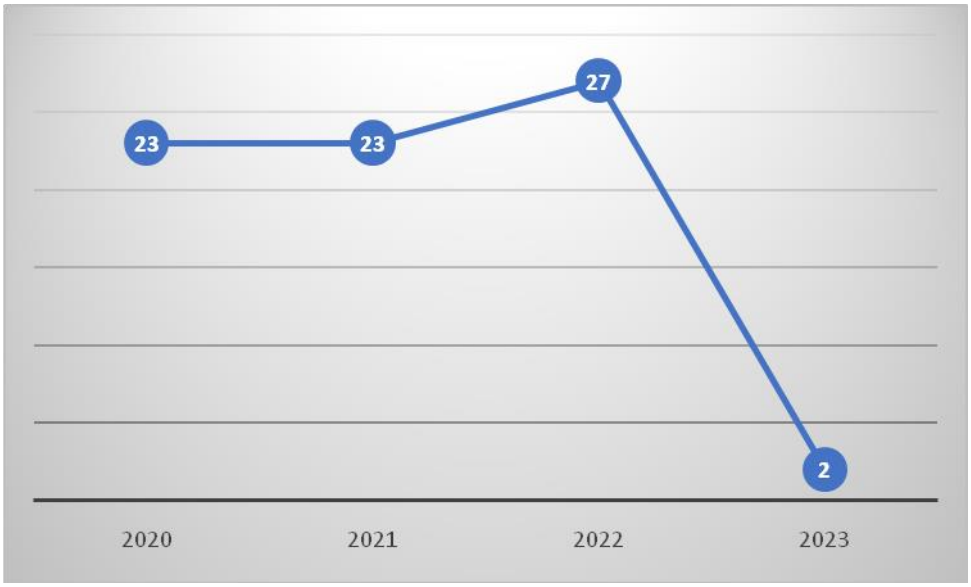
Tabel 1 menjelaskan terkait objek penelitian dari artikel yang menjadi sampel dalam penelitian ini. Terdapat 20 bidang yang menjadi objek penelitian. Bidang kredit menjadi bidang dengan jumlah terbanyak yang dijadikan objek penelitian yakni sebanyak 23 artikel yang membahas terkait teknik atau model deteksi *fraud* dalam bidang kredit. Posisi kedua diisi oleh bidang *systematic literature review* sebanyak 10 artikel yang membahas terkait teknik atau model deteksi *fraud* dalam kajian literatur. Kemudian bidang asuransi kesehatan sebanyak 7 artikel, laporan keuangan sebanyak 6 artikel, perbankan 5 artikel, bursa efek 3 artikel, asuransi 3 artikel kemudian asuransi mobil, *online adversiting*, konsultan investasi dan pinjaman masing-masing 2 artikel.

Bidang Asuransi Properti, kesehatan, *cyber phising*, Perpajakan, *Shell Company*, Program Sosial, skema Ponzi dan *Supply chain* masing-masing 1 artikel.



Gambar 1. Metode Penelitian

Sumber: Diolah oleh peneliti, 2023



Gambar 2. Tingkat Publikasi Pertahun

Sumber: Diolah oleh peneliti, 2023

Nomor	Objek Penelitian	Jumlah
1	Asuransi	3
2	Asuransi Kesehatan	7
3	Asuransi Mobil	2
4	Asuransi Properti	1
5	Bursa Efek	3
6	*cyber phising*	1
7	*e-commerce*	2
8	Kesehatan	1
9	Konsultan investasi	2
10	Kredit	23
11	Laporan Keuangan	6
12	*online advertising*	2
13	Perpajakan	1
14	Perbankan	5
15	*Shell Company*	1
16	Pinjaman	2
17	Program Sosial	1
18	SLR	10
19	Skema Ponzi	1
20	*Supply chain*	1
	Jumlah	**75**

Tabel 1. Objek Penelitian

Sumber: Diolah oleh peneliti, 2023

Teknik atau model deteksi *fraud* yang digunakan oleh para peneliti dijelaskan pada gambar Tabel 2. Berdasarkan hasil analisis terdapat 24 teknik atau model yang digunakan oleh peneliti dalam melakukan deteksi *fraud*. Beberapa peneliti menggunakan beberapa teknik atau model dalam satu jurnal. Kemudian beberapa peneliti lainnya melakukan metode SLR (*SystematicLiterature Review)* yang bertujuan untuk melakukan analisis atas teknik-teknik yang digunakan oleh peneliti-peneliti sebelumnya dalam mendeteksi *fraud*.

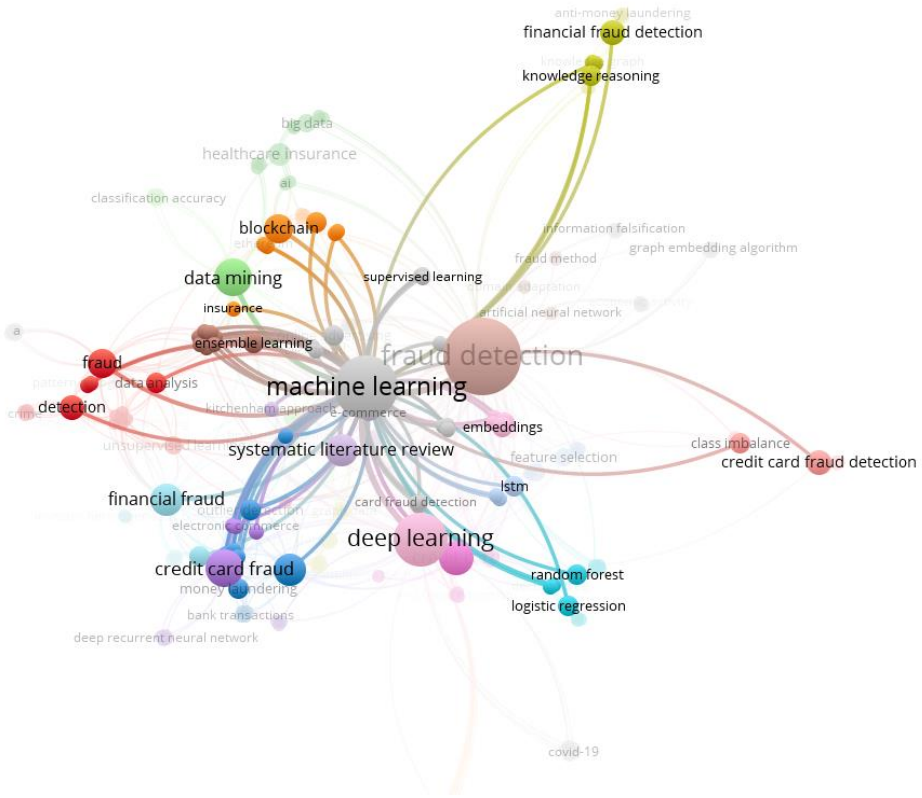
Hasil menunjukkan bahwa teknik *machine learning* menjadi teknik terpopuler yang digunakan oleh peneliti yakni sebanyak 30 artikel menggunakan teknik tersebut. Kemudian diikuti oleh teknik *deep learning* sebanyak 12 artikel , *systematic literature review* sebanyak 10 artikel, *Artificial intelligence* sebanyak 3 artikel dan teknik lainnya masing-masing 01 artikel seperti yang dijelaskan pada tabel 2.

Nomor	Teknik	Jumlah
1	*A Hybird Data Mining*	1
2	*Artificial Intelligence*	3
3	*Deep Learning*	12
4	*Dynamic Social Network*	1
5	*Hidden Markov Model (HMM)*	1
6	*Harris water optimization-based deep recurrent neural network (HWO-RNN)*	1
7	*Generative Adversarial Networks (GANs)*	1
8	*Hierarchical Multi-task Learning*	1
9	*Long Short Term Memory (LSTM)*	1
10	*Machine Learning*	30
11	*Meta-Learning*	1
12	*Weighted Extreme Learning Machine*	1
13	*Multiple Classifiers System (MCS)*	1
14	*MapReduce*	1
15	*Sequence Rule Engine And Prediction Based Engine*	1
16	*Newcomb–Benford's Law (NBL*	1
17	*Subgraph-Based Graph Neural Network (SubGNN*	1
18	*Novel Hybrid Method*	1
19	*Related-Party Transactions (RPTs*	1
20	*Transfer Learning*	1
21	*Quantum Machine Learning (QML)*	1
22	*Quantum Support Vector Machine (QSVM)*	1
23	*Peer-Effect-Based*	1
24	*SLR*	10
	Jumlah	**75**

Tabel 2. Teknik Deteksi Fraud

Sumber: Diolah oleh peneliti, 2023

Analisis Bibliometrik VOSviewer



Gambar 3. Output VOSviewer

Output VOSviewer menunjukkan bahwadeteksi *fraud* paling populer menggunakan *machine learning* dan *deep learning* sedangkan bidang deteksi paling populer adalah bidang kredit. Berdasarkan hal tersebut maka untuk penelitian selanjutnya bisa menggunakan bidang lain seperti Asuransi Properti, kesehatan, *cyber phising*, Perpajakan, *Shell Company*, Program Sosial, skema Ponzi dan *Supply chain* karena hanya terdapat1 artikel untuk masing-masing bidang tersebut.

SystematicLiterature Review

Tabel 3, 4, 5, dan 6 merupakan kajian pustaka atas jurnal-jurnal yang diperoleh dalam proses *purposive Sampling*. Kajian pustaka berisi nama peneliti beserta tahun publikasi jurnal, *database* publikasi dan temuan dari artikel-artikel tersebut.

Tahun 2020

No	Peneliti	Sumber	Temuan
01	(Chen et al., 2020)	ScienceDirect	Penggunaan model Logistic Regression dan Hybrid Credit Scoring Model meningkatkan akurasi dalam skor kredit. Pengingkatan skor kredit dapat mengurangi terjadinya penipuan kredit
02	(Sahni et al., 2020)	ScienceDirect	Hasil menunjukkan bahwa solusi yang diusulkan (Deep Learning, Computer Vision, Internet of Things, Image Processing, Semantic Segmentation, Feature Extraction) memiliki akurasi 97%,yang dapat ditingkatkan lebih lanjut dengan kumpulan data yang disempurnakan yang didedikasikan hanya untuk deteksi penipuan.
03	(Bagga et al., 2020)	ScienceDirect	Peneliti melakukan perbandingan model Logistic Regression, Naive Bayes, K nearest neighbours, Multi Layer Perceptron, Ada Boost, Quadrant Discriminant Analysis, Random Forests, Pipelining dan Ensemble Learning dalam mendeteksi fraud transaksi kartu kredit. Hasil penelitian menunjukkan bahwa model Pipelining adalah yang terbaik.
04	(Olowookere & Adewale, 2020)	ScienceDirect	Kerangka meta-learning ensemble efisien dalam menghasilkan meta-klasifikasi yang secara efektif mendeteksi transaksi penipuan di berbagai database sistem pembayaran terlepas dari proporsi yang tersedia
05	(Vanhoeyveld et al., 2020)	ScienceDirect	Metode anomaly detection techniques efektif dalam mendeteksi kasus penipuan perpajakan
06	(Craja et al., 2020)	ScienceDirect	Model deep learning efektif dalam deteksi fraud laporan keuangan
07	(Lucas et al., 2020)	ScienceDirect	Hidden Markov Model (HMM) adalah alat yang ampuh dan terbukti menghadirkan properti menarik untuk deteksi penipuan.
08	(Yan et al., 2020)	ScienceDirect	Artificial bee colony algorithm dapat diterapkan untuk mendeteksi penipuan asuransi mobil
09	(Zhu et al., 2020)	ScienceDirect	Weighted Extreme Learning Machine menunjukkan kinerja deteksi yang tinggi.
10	(Pourhabibi et al., 2020)	ScienceDirect	Pendekatan systematic literature review terkait Model Graph- Basedanomaly Detection dalam deteksi fraud
11	(Vaughan, 2020)	ScienceDirect	big data model efektif dalam deteksi credit card fraud
12	(Omair & Alturki, 2020)	IEEE	Pendekatan systematic literature review terkait Process-based fraud (PBF) dalam deteksi fraud
13	(Kalid et al., 2020)	IEEE	Model Multiple Classifiers System (MCS) menunjukkan kinerja deteksi yang tinggi.

14	(Dhieb et al., 2020)	IEEE	Penggunaan machine learning (SISBAR, XGBoost, VFDT algorithms), klasifikasi yang diusulkan tidak hanya memastikan yang akurasi terbaik dalam mendeteksi klaim penipuan tetapi juga dapat mengklasifikasikan berbagai jenis penipuan untuk asuransi berbeda dengan solusi yang ada.
15	(Taha & Malebary, 2020)	IEEE	Penggunaan machine learning; optimized light gradient boosting machine (OLightGBM). Pendekatan yang diusulkan mengungguli pembelajaran mesin lainnya dalam deteksi fraud.
16	(Zhou et al., 2020)	IEEE	Penggunaan model MapReduce, Eksperimen menunjukkan bahwa metode ini memiliki kinerja yang lebih baik daripada beberapa metode benchmark.
17	(Matloob et al., 2020)	IEEE	Penggunaan metodologi Sequence rule engine and Prediction based engine. Berbagai eksperimen telah dilakukan untuk memvalidasi penerapan metodologi yang dikembangkan dan hasilnya menunjukkan bahwa metodologi ini relevan untuk mendeteksi penipuan perawatan kesehatan dan memberikan akurasi rata-rata 85%
18	(Karadayi et al., 2020)	IEEE	Penggunaan hybrid deep learning menunjukkan peningkatan yang signifikan pada kinerja deteksi anomali tanpa pengawasan bahkan di kenario rasio kelangkaan data dan kontaminasi tinggi (di mana rasio anomali dalam kumpulan data lebih dari 5%).
19	(Tingfei et al., 2020)	IEEE	Hasil eksperimen menunjukkan bahwa metode variational automatic coding (VAE) berkinerja baik dalam deteksi fraud kredit.
20	(Rai, 2020)	IEEE	Temuan menunjukkan bahwa Neural Network (NN) based unsupervised learning meghasilkan akurasi 99,87% dalam deteksi fraud kredit
21	(Song, 2020)	IEEE	Temuan menunjukkan bahwa a hybird datamining meghasilkan akurasi 98,5% dalam deteksi fraud E-Bank
22	(Jullum et al., 2020)	Emerald	Pendekatan machine learning (XGBoost) unggul dalam deteksi money laundring
23	(Kolli & Tatavarthi, 2020)	Emerald	Harris water optimization-based deep recurrent neural network (HWO-RNN) memperoleh kinerja yang lebih baik dalam hal metrik, seperti akurasi, sensitivitas, dan spesifisitas dengan nilai 0,9192, 0,7642, dan 0,9943.

Tabel 3. Literature Review

Tahun 2021

No	Peneliti	Sumber	Temuan
01	(Sánchez-Aguayo et al., 2021)	MDPI	Pendekatan *systematic literature review*. Temuan menunjukkan bahwa sebagian besar penelitian menggunakan *machine learning techniques* dalam deteksi *fraud*
02	(Thaifur et al., 2021)	ScienceDirect	Metode yang tepat untuk digunakan dalam mendeteksi penipuan adalah *secondary data tracking*, penyediaan informasi, dan spesialis teknologi.
03	(Lee & Cho, 2021)	ScienceDirect	Model yang diusulkann berkontribusi dalam proses deteksi, akan tetapi perlu perbaikan dalam kasus penyalahgunaan pengobatan
04	(Zhu et al., 2021)	ScienceDirect	*Artificial intelligence* (AI) digunakan dalam deteksi fraud laporan keuangan
05	(Severino & Peng, 2021)	ScienceDirect	Temuan menunjukkan bahwa *machine learning* yakni *ensemble-based method*(*random forest and gradient boosting*) dan *deep neural networks* menunjukkan hasil yang terbaik dibandingkan dengan pengklasifikasi lainnya, termasuk yang umum seperti regresi logistik dalam deteksi *fraud* di asuransi properti
06	(Forough & Momtazi, 2021)	ScienceDirect	Hasil eksperimen menunjukkan bahwa model*Ensemble of Deep Sequential* yang diusulkan mengungguli model mutakhir model dalam semua kriteria evaluasi. Selain itu, analisis waktu yang diusulkan menunjukkan bahwa model ini lebih efisien dalam hal kinerja dibandingkan dengan model terbaru di lapangan dalam deteksi *fraud credit card*
07	(Błaszczyński et al., 2021)	ScienceDirect	Temuan menunjukkan bahwa *machine learning* yakni *Dominancebased Rough Set Balanced Rule Ensemble* (DRSA-BRE*)* lebih unggul daripada teknik tradisional dalam mendeteksi *fraud* pinjaman
08	(Azevedo et al., 2021)	ScienceDirect	Metode *Newcomb–Benford's Law* (NBL) dapat menjadi metode yang tepat untuk penyelidikan penipuan atas manfaat program distribusi kesejahteraan sosial dengan pembayaran penerima manfaat dikelompokkan secara geografis.

09	(Fan et al., 2021)	ScienceDirect	*machine learning* berupa *anti-leakage smart Ponzi schemes detection* (Al-SPSD) kompetitif dan efektif serta andal dalam mendeteksi skema Ponzi
10	(Song et al., 2021)	ScienceDirect	*subgraph-based Graph neural network* (SubGNN) ketepatannya lebih tinggi dari 0:99 dan lebih dari 90% sampel penipuan dapat dideteksi
11	(Wu et al., 2021)	ScienceDirect	Temuan menunjukkan bahwa *random forest algorithm* lebih unggul dibanding *bipartite graph propagation algorithm* dalam mendeteksi *fraud online advertising*
12	(Koreff et al., 2021)	ScienceDirect	*Data analytics* (ab) memiliki konsekuensi negatif dalam proses deteksi *healthcare fraud audit*
13	(Zhang et al., 2021)	ScienceDirect	*Deep learning* berupa *homogeneity-oriented behavior analysis*(HOBA) terbukti efisien dalam mendekteksi *fraud credit card*
14	(Al-Hashedi & Magalingam, 2021)	ScienceDirect	studi menunjukkan bahwa 34 teknik *data mining* digunakan untuk mengidentifikasi penipuan di berbagai bidang keuangan. SVM ditemukan sebagai salah satu teknik deteksi penipuan keuangan yang paling banyak digunakan sekitar 23% dari keseluruhan penelitian, diikuti oleh Na Bay 15%. Hasil tinjauan komprehensif mengungkapkan bahwa sebagian besar teknik *data mining* diterapkan secara ekstensif pada penipuan bank dan penipuan asuransi dengan total 61 studi penelitiandari 75 yang merupakan porsi terbesar sama dengan 81,33%.
15	(Barraclough et al., 2021)	ScienceDirect	Penggunaan *machine learning* berupa *blacklist-based, web content-based and heuristic based approaches* dapat dapat mendeteksi *cyber phising* dengan akurasi tinggi
16	(Li et al., 2021)	ScienceDirect	*novel hybrid method* mampu mendeteksi *fraud credit card*
17	(Mao, 2021)	ScienceDirect	*Related-Party Transactions* (RPTs) meningkatkan kinerja deteksi penipuan keuangan di Bursa Efek
18	(Gomes et al., 2021)	Wiley	Penggunaan model *deep learning* memberikan kinerja yang luar bisa dalam deteksi *fraud* dalam bidang asuransi
19	(Zhou et al.,	IEEE	*Big Data approach* digunakan dalam implementasi *graph embedding algorithm* Node2Vec, temuan

	2021)		menunjukkan bahwa metode tersebut meningkatkan efisiensi deteksi penipuan laporan keuangan
20	(Ileberi et al., 2021)	IEEE	*machine learning* berupa *Adaptive Boosting* (AdaBoost) *technique* berdampak positif pada deteksi *fraud credit card*
21	(Abidi et al., 2021)	IEEE	*machine learning* berupa *Support vector machine* (SVM), dan *Artificial neural network* (ANN) memiliki akurasi sebesar 99, 63% dalam mendeteksi *fraud*
22	(Lebichot et al., 2021)	IEEE	Metode *Transfer learning* akurat dalam mendeteksi *fraud credit card*
23	(El Naby et al., 2021)	IEEE	*deep learning* berupa OSCNN (*Over Sampling with dan Convolution Neural Network*) dan MLP (*Multi-layer perceptron*) mencapai hasil yang lebih baik dengan akurasi 98%.

Tabel 4. Literature Review

Tahun 2022

No	Peneliti	Sumber	Temuan
01	(Ali et al., 2022)	MDPI	Hasil *review* menunjukkan bahwa teknik *Machine Learning* paling populer digunakan untuk deteksi penipuan. *support vector machine* (SVM) dan *artificial artificial neural network* (ANN) adalah algoritma *Machine Learning* (ML) populer yang digunakan untuk mendeteksi penipuan
02	(Rodrigues et al., 2022)	ScienceDirect	Temuan utama studi menunjukkan bahwa dari 64 artikel, hanya lima yang berfokus pada masalah pencegahan penipuan, dan penipuan kartu kredit merupakan jenis penipuan yang paling banyak dieksplorasi. Selain itu, literatur saat ini kekurangan studi yang mengusulkan strategi untuk mendeteksi penipuan
03	(Wang et al., 2022)	ScienceDirect	Setelah mempertimbangkan indikator keyakinan heterogen investor, penipuan keuangan dapat diidentifikasi menggunakan enam model *machine learning* yakni *logistic regression, support vector machine, decision tree, random forest, naive Bayesian, and artificial neural network*
04	(Amponsah et	ScienceDirect	Penggunaan *machine learning techniques* dan *blockchain*

	al., 2022)		*technology* memiliki akurasi sebesar 97,96% dala mmendeteksi *fraud* asuransi kesehatan
05	(Hilal et al., 2022)	ScienceDirect	*generative adversarial networks* (GANs) populer digunakan dalam deteksi *fraud credit card* dan asuransi. Model *deep learningberupa convolutional neural networks* (CNNs) dan *long short-term memory networks* (LSTMs) populer dalam deteks*i fraud credit card*
06	(Lokanan & Sharma, 2022)	ScienceDirect	*Machine learning* berupa *Logistic regression, ecision Tree Classifier (DTC), andom Forests Classifier (RFC), CatBoast, Hyperparameter tuning with GridSearchCV (GSCV)* efektif dalam mendeteksi *fraud*
07	(Rocha-Salazar et al., 2022)	ScienceDirect	atribut badan hukum dan memasukkan perbandingan diri dan kelompok ke dalam *dynamic social network* menghasilkan akurasi seimbang dan *true positive rate* masing-masing di atas 0,9 dan 0,85 dalam deteksi *shell companies*
08	(Chen et al., 2022)	ScienceDirect	*hierarchical multi-task learning* efektif dalam deteksi penipuan pinjaman
09	(Seify et al., 2022)	ScienceDirect	*Machine learning* bermanfaat dalam mendeteksi faktur yang tidak tepat dalam *supply chain*
10	(Goecks et al., 2022)	Wiley	*Literature review* terkait *anti-money laundering* (AML) dan *financial fraud detection* (FFD)
11	(Alarfaj et al., 2022)	IEEE	*Machine Learning* dan *Deep Learning Algorithms*efektif untuk pendeteksian *fraud* kredit
12	(Nguyen et al., 2022)	IEEE	model yang di usulkan bekerja dengan baik dalam deteksi fraud dengan skor AUC sebesar 0,97 (Cat Boost) dan 0,84 (Deep Neural Network).
13	(Xiuguo & Shengyong, 2022)	IEEE	*Machine Learning* berupa *long short-term memory* (LSTM) *Gated Recurrent Unit* (GRU) efektif dalam deteksi fraud Bursa Efek China
14	(Batool & Byun, 2022)	IEEE	Model *ensemble learning* efektif dalam deteksi *fraud Online advertising*
15	(Dumitrescu et al., 2022)	IEEE	Membangun metode deteksi anomali dalam transaksi *money laundering*
16	(Kapadiya et al., 2022)	IEEE	*Artificial Intelligence* (AI) efektif dalam deteksi *fraud* asuransi kesehatan

17	(Pranto et al., 2022)	IEEE	Blockchain dan *Machine Learning* efektif dalam deteksi *fraud*
18	(Esenogho et al., 2022)	IEEE	*Long shortterm memory* (LSTM) unggul dalam deteksi *fraud credit card*
19	(Hashemi et al., 2023)	IEEE	*Bayesian optimization* dan *deep learning* menunjukkan bahwa keduanya merupakan metode yang mutakhir dalam deteksi *fraud* di perbankan
20	(Wang et al., 2022)	IEEE	Aplikasi *quantum machine learning* (QML) memiliki potensi yang baik dalam deteksi *fraud*
21	(Grossi et al., 2022)	IEEE	*quantum support vector machine* (QSVM) memilik peningkatan akurasi dalam deteksi *fraud*
22	(Fursov et al., 2022)	IEEE	*deep learning* efektif dalam deteksi *fraud* asuransi kesehatan
23	(Benedek et al., 2022)	Emerald	Studi literatur ini menemukan bahwa deteksi penipuan asuransi mobil sedang mengalami transformasi, di mana metode deteksi berbasis statistik tradisional digantikan oleh pendekatan berbasis data mining dan *Artificial Intelligence*
24	(Westland, 2022)	Emerald	Bayesian A/B tidak hanya menghasilkan penggambaran yang jelas tentang waktu dan dampak dari penipuan, tetapi menghitung hilangnya dolar penjualan, lalu lintas, dan waktu di situs web perusahaan, dengan batas kepercayaan yang tepat. Pengujian A/B mengidentifikasi penipuan dalam rasio signifikansi 5%.
25	(Farbmacher et al., 2022)	ScienceDirect	*deep neural network* efektif dalam deteksi fraud asuransi kesehatan
26	(Xia et al., 2022)	Wiley	*peer-effect-based* terbukti efisien dalam mendeteksi *fraud* di Bursa Efek China
27	(Ashtiani & Raahemi, 2022)	IEEE	Pendekatan *systematic literature review* terkait Model *machine learning* dan *Data Mining* dalam deteksi *fraud*

Tabel 5. Literature Review

Tabel 6. Literature Review

Tahun 2023			
No	**Peneliti**	**Sumber**	**Temuan**
01	(Cherif et al., 2023)	ScienceDirect	Studi kami menunjukkan penyelidikan terbatas sampai saat ini dalam *deep learning*, mengungkapkan bahwa diperlukan lebih banyak penelitian untuk mengatasi tantangan yang terkait dengan mendeteksi penipuan kartu kredit melalui penggunaan teknologi baru seperti *big data analytics*, *large-scale machine learning*dan *cloud computing*
02	(Afriyie et al., 2023)	ScienceDirect	*Machine learning models: logistic regression, random forest, and decision trees to classify, random forest* merupakan model terbaik denga akurasi 96%.

Jenis penelitian *literature review* menunjukkan bahwa teknik *data mining* digunakan untuk mengidentifikasi penipuan di berbagai bidang keuangan seperti *credit card*, asuransi, bitcoin dan laporan keuangan (Al-Hashedi & Magalingam, 2021). Sedangkan (Rodrigues et al., 2022) Menunjukkan bahwa dari 64 artikel, hanya lima yang berfokus pada masalah pencegahan penipuan, dan penipuan kartu kredit merupakan jenis penipuan yang paling banyak dieksplorasi. Selain itu, literatur saat ini kekurangan studi yang mengusulkan strategi untuk mendeteksi penipuan. Penelitian untuk mengatasi tantangan yang terkait dengan mendeteksi penipuan kartu kredit masih terbatas pada teknik *deep learning* dan diperlukan penelitian lebih banyak melalui penggunaan teknologi baru seperti *big data analytics*, *large-scale machine learning*dan *cloud computing* (Cherif et al., 2023).

Metode eksperimen menunjukkan bahwa model yang diusulkan oleh para peneliti efektif dalam deteksi *fraud*. Penggunaan *deep learning*, *Machine learning, artificial intelligence, MapReduce*, *Sequence rule engine and Prediction based engine, Data analytics* (ab)dan *data mining* terbukti efektif dalam deteksi *fraud* di bidang asuransi secara umum dan asuransi secara khusus seperti asuransi mobil, asuransi properti dan asuransi kesehatan (Dhieb et al., 2020; Farbmacher et al., 2022; Fursov et al., 2022; Gomes et al., 2021; Kapadiya et al., 2022; Koreff et al., 2021; Lee & Cho, 2021; Matloob et al., 2020; Severino & Peng, 2021; Westland, 2022; Yan et al., 2020; Zhou et al., 2021).

Machine learning, *deep learning, Related-Party Transactions* dan *peereffectbased* efektif dalam deteksi *fraud* di Bursa Efek (Xia et al., 2021; Xiuguo & Shengyong, 2022).*Machine learning* juga efektif dalam deteksi *cyber phising* (Barraclough et al., 2021). *Subgraph-based Graph neural network*(SubGNN), *machine learning* berupa *Support vector machine* (SVM), *Artificial neural network* (ANN) dan Bayesian A/B efektif dalam deteksi e-*commerce fraud* sedangkan *ensemble learning* efektif dalam deteksi *fraud online adversiting* (Abidi et al., 2021; Batool & Byun, 2022; Song et al., 2021).

Deteksi *fraud* di bidang laporan keuangan efektif menggunakan *deep learning, machine learning, Data Mining, artificial intelligence, graph embedding algorithm, quantum machine learning (QML),* dan *quantum support vector machine (QSVM)* (Ali et al., 2019; Craja et al., 2020; Goecks et al., 2022; Grossi et al., 2022; Pranto et al., 2022; Wang et al., 2022; Zhou et al., 2020; Zhu et al., 2021).

Model *anomaly detection techniques* dalam deteksi *fraud* bidang perpajakan(Vanhoeyveld et al., 2020). Deteksfi *fraud* perbankan efektif menggunakan*hybird data mining, machine learning, Water wave optimization (WWO)* , *Bayesian optimization dan deep learning* (Dumitrescu et al., 2022; Hashemi et al., 2023; Jullum et al., 2020; Kolli & Tatavarthi, 2020).

Deteksi *shell company* efektif menggunakan *dynamic social network* (Rocha-Salazar et al., 2022). Deteksi fraud pinjaman efektif menggunanakan *machine learning* dan *hierarchical multi-task learning* (Błaszczyński et al., 2021; Chen et al., 2022).Metode *Newcomb–Benford's Law* (NBL) dalam deteksi fraud program sosial (Azevedo et al., 2021). *machine learning* kompetitif dan efektif serta andal dalam mendeteksi skema Ponzi dan *supply chain* (Fan et al., 2021).

Deteksi *fraud* di bidang kredit merupakan bidang yang paling banyak diteliti dari tahun 2020 hingga 2023. Model deteksi *fraud* kredit efektif menggunakan *deep learning* dan *machine learning* seperti *Logistic regression, pipeling*&*en-semble learning, Meta-learning, multi-perspective HMMs, big data model, Weighted Extreme Learning Machine, Data mining technique, Unsupervised Learning, dan domain adaptation/Transfer learning* (Afriyie et al., 2023; Al-Hashedi & Magalingam, 2021; Alarfaj et al., 2022; Chen et al., 2022; Cherif et al., 2023; El Naby et al., 2021; Esenogho et al., 2022; Forough & Momtazi, 2021; Hilal et al., 2022; Ileberi et al., 2021; Kalid et al., 2020; Lebichot et al., 2021; Li et al., 2021; Lucas et al., 2020; Olowookere & Adewale, 2020; Taha & Malebary, 2020; Tingfei et al., 2020; Vaughan, 2020; Zhang et al., 2021; Zhu et al., 2021).

Berdasarkan hasil penelitian di atas ditemukan bahwa tren topik terkait deteksi dan investigasi *fraud* yang paling banyak ada di bidang kredit. Seperti yang disebutkan oleh (Dornadulaa & Sa, 2019) penipuan kartu kredit merupakan sasaran empuk. Tanpa risiko apa pun, jumlah yang signifikan dapat ditarik tanpa sepengetahuanpemiliknya. Penipu selalu berusaha membuat setiap transaksi penipuan menjadi sah, yangmembuat deteksi penipuan menjadi sangat menantang dan sulit untuk dideteksi.

Pada tahun 2017, terdapat 1.579 pelanggaran data dan hampir 179 juta catatan di antaranya merupakan penipuan kartu kredit dengan 133.015 laporan, kemudian penipuan terkait pajak dengan 82.051 laporan, penipuan telepon dengan 55.045 laporan, diikuti oleh penipuan bank dengan 50.517 laporan (Dornadulaa & Sa, 2019). Dalam laporan tersebut ditemukan bahwa penipuan bidang perpajakan berada di posisi kedua terbanyak yakni sebanyak 82.051 laporan, akan tetapi temuan dalam penelitian ini menunjukkann bahwa penelitian terkait deteksi*fraud* bidang perpajakan hanya terdapat 01 artikel selama periode 2020 hingga 2013. Hal tersebut memungkinkan peneliti selanjutnya menggali lebih jauh terkait topik *fraud* bidang perpajakan.

Selain bidang perpajakan, penipuan di bidang layanan kesehatan adalah masalah global yang memengaruhi negara berkembang dan negara maju. Di seluruh dunia, sejumlah besar uang hilang karena penipuan dalam bidang kesehatan (Amponsah et al., 2022). Akan tetapi, temuan dalam penelitian ini menunjukkan bahwa artikel terkait bagaimana deteksi *fraud* dalam layanan kesehatan hanya terdapat 01 artikel saja. Peluang bagi peneliti selanjutnya dapat melakukan penelitian tentang bagaimana cara mendeteksi tindakan *fraud* di bidang kesehatan, Misalnya bagaimana cara mendeteksi tindakan *fraud* dalam Jaminan Kesehatan Nasional (JKN).

Temuan-temuan di atas dapat memberikan gambaran kepada peneliti selanjutnya dalam melakukan penelitian terkait deteksi dan investigasi *fraud*. Teknik-teknik yang digunakan dalam proses penelitian dapat disesuaikan dengan objek atau bidang yang akan diteliti karena setiap teknik memiliki keunggulan dan kelemahan masing-masing.

SIMPULAN

Perkembangan penelitian terkait deteksi dan ivestigasi *fraud*dipetakan dalam beberapa kategori. Database Science Direct (SD) merupakan database terbanyak dalam publikasi artikel yang membahas deteksi dan investigasi *fraud*selama periode 2020-2023 yaknisebanyak 38artikel. Tren publikasi menunjukkan bahwa tahun 2022 merupakan tahun terbanyak dalam perilisan publikasi yakni sebanyak 28 artikel. Metode penelitian terpopuler menggunakan metode eksperimen. Hal tersebut didasari karena sebagian besar penelitian menggunakan teknologi dalam proses deteksi dan investigasi *fraud*.

Hasil *output* VOSviewer menyajikan informasi kebaruan penelitian sehingga dapat memberikan kemudahan kepada peneliti selanjutnya dalam melakukan riset terkait deteksi *fraud*. Hasil menunjukkan bahwa teknik yang digunakan dalam deteksi *fraud* paling populer menggunakan *machine learning* dan *deep learning*, kemudian bidang yang paling banyak diteliti adalah *credit card*. Berdasarkan informasi tersebut peneliti selanjutnya bisa menggunakan bidang lain seperti Asuransi Properti, kesehatan, *cyber phising*, Perpajakan, *Shell Company*, Program Sosial, skema Ponzi dan *Supply chain* karena hanya terdapat 01 artikel untuk masing-masing bidang tersebut.

Proses pemetaan data dalam penelitian ini masih menggunakan cara manual yakni menggunakan microsoft excel. *Software* VOSviewer hanya digunakan untuk melihat kebaruan penelitian terkait deteksi dan investigasi *fraud* karena dalam prosesnya beberapa database tidak dapat diintegrasikan dalam *software* tersebut. Penelitian selanjutnya bisa menggunakan *software* lainnya seperti R-*studio* dalam mengolah dan memetakan data. Peneliti selanjutnya juga bisa menambah jumlah periode penelitian serta menambah jumlah database untuk mengetahui secara lebih luas lagi bagaimana perkembangan penelitian terkait deteksi dan investigasi *fraud*.

DAFTAR PUSTAKA

Abidi, W. U. H., Daoud, M. S., Ihnaini, B., Khan, M. A., Alyas, T., Fatima, A., & Ahmad, M. (2021). Real-Time Shill Bidding Fraud Detection Empowered With Fussed Machine Learning. *IEEE Access, 9*, 113612-113621. https://doi.org/10.1109/access.2021.3098628

ACFE. (2022). Occupational Fraud 2022: A Report to The Nations.

Afriyie, J. K., Tawiah, K., Pels, W. A., Addai-Henne, S., Dwamena, H. A., Owiredu, E. O., Ayeh, S. A., & Eshun, J. (2023). A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. *Decision Analytics Journal, 6*. https://doi.org/10.1016/j.dajour.2023.100163

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

Alarfaj, F. K., Malik, I., Khan, H. U., Almusallam, N., Ramzan, M., & Ahmed, M. (2022). Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms. *IEEE Access, 10*, 39700-39715. https://doi.org/10.1109/access.2022.3166891

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. *Applied Sciences, 12*(19). https://doi.org/10.3390/app12199637

Ali, M. A., Azad, M. A., Parreno Centeno, M., Hao, F., & van Moorsel, A. (2019). Consumer-facing technology fraud: Economics, attack methods and potential solutions. *Future Generation Computer Systems, 100*, 408-427. https://doi.org/10.1016/j.future.2019.03.041

Amponsah, A. A., Adekoya, A. F., & Weyori, B. A. (2022). A novel fraud detection and prevention method for healthcare claim processing using machine learning and blockchain technology. *Decision Analytics Journal, 4*. https://doi.org/10.1016/j.dajour.2022.100122

Ashtiani, M. N., & Raahemi, B. (2022). Intelligent Fraud Detection in Financial Statements Using Machine Learning and Data Mining: A Systematic Literature Review. *IEEE Access, 10*, 72504-72525. https://doi.org/10.1109/access.2021.3096799

Azevedo, C. d. S., Gonçalves, R. F., Gava, V. L., & Spinola, M. d. M. (2021). A Benford's Law based methodology for fraud detection in social welfare programs: Bolsa Familia analysis. *Physica A: Statistical Mechanics and its Applications, 567*. https://doi.org/10.1016/j.physa.2020.125626

Bagga, S., Anish, G., Gupta, N., & Goyal, A. (2020). Credit Card Fraud Detection using Pipeling and Ensemble Learning. *Procedia Computer Science, Volume 173, 2020, Pages 104-112*. https://doi.org/https://doi.org/10.1016/j.procs.2020.06.014

Barraclough, P. A., Fehringer, G., & Woodward, J. (2021). Intelligent cyber-phishing detection for online. *Computers & Security, 104*. https://doi.org/10.1016/j.cose.2020.102123

Batool, A., & Byun, Y.-C. (2022). An Ensemble Architecture Based on Deep Learning Model for Click Fraud Detection in Pay-Per-Click Advertisement Campaign. *IEEE Access, 10*, 113410-113426. https://doi.org/10.1109/access.2022.3211528

Benedek, B., Ciumas, C., & Nagy, B. Z. (2022). Automobile insurance fraud detection in the age of big data – a systematic and comprehensive literature review. *Journal of Financial Regulation and Compliance, 30*(4), 503-523. https://doi.org/10.1108/JFRC-11-2021-0102

Błaszczyński, J., de Almeida Filho, A. T., Matuszyk, A., Szeląg, M., & Słowiński, R. (2021). Auto loan fraud detection using dominance-based rough set approach versus machine learning methods. *Expert Systems with Applications, 163*. https://doi.org/10.1016/j.eswa.2020.113740

Chen, K., Yadaw, A., Khan, A., & Zhu, K. (2020). Credit Fraud Detection Based on Hybrid Credit Scoring Model. *International Conference on Computational Intelligence and Data Science (ICCIDS 2019)* https://doi.org/https://doi.org/10.1016/j.procs.2020.03.176

Chen, L., Jia, N., Zhao, H., Kang, Y., Deng, J., & Ma, S. (2022). Refined analysis and a hierarchical multi-task learning approach for loan fraud detection. *Journal of*

Management Science and Engineering, 7(4), 589-607. https://doi.org/10.1016/j.jmse.2022.06.001

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. *Journal of King Saud University - Computer and Information Sciences, 35*(1), 145-174. https://doi.org/10.1016/j.jksuci.2022.11.008

Craja, P., Kim, A., & Lessmann, S. (2020). Deep learning for detecting financial statement fraud. *Decision Support Systems, 139*. https://doi.org/10.1016/j.dss.2020.113421

Dhieb, N., Ghazzai, H., Besbes, H., & Massoud, Y. (2020). A Secure AI-Driven Architecture for Automated Insurance Systems: Fraud Detection and Risk Measurement. *IEEE Access, 8*, 58546-58558. https://doi.org/10.1109/access.2020.2983300

Dornadulaa, V. N., & Sa, G. (2019). Credit Card Fraud Detection using Machine Learning Algorithms. *Procedia Computer Science 165 (2019) 631–641.* https://doi.org/10.1016/j.procs.2020.01.057

Dumitrescu, B., Baltoiu, A., & Budulan, S. (2022). Anomaly Detection in Graphs of Bank Transactions for Anti Money Laundering Applications. *IEEE Access, 10*, 47699-47714. https://doi.org/10.1109/access.2022.3170467

El Naby, A. A., El-Din Hemdan, E., & El-Sayed, A. (2021). *Deep Learning Approach for Credit Card Fraud Detection* 2021 International Conference on Electronic Engineering (ICEEM),

Esenogho, E., Mienye, I. D., Swart, T. G., Aruleba, K., & Obaido, G. (2022). A Neural Network Ensemble With Feature Engineering for Improved Credit Card Fraud Detection. *IEEE Access, 10*, 16400-16407. https://doi.org/10.1109/access.2022.3148298

Fan, S., Fu, S., Xu, H., & Cheng, X. (2021). Al-SPSD: Anti-leakage smart Ponzi schemes detection in blockchain. *Information Processing & Management, 58*(4). https://doi.org/10.1016/j.ipm.2021.102587

Farbmacher, H., Löw, L., & Spindler, M. (2022). An explainable attention network for fraud detection in claims management. *Journal of Econometrics, 228*(2), 244-258. https://doi.org/10.1016/j.jeconom.2020.05.021

Flegel, U., Vayssière, J., & Bitz, G. (2010). A State of the Art Survey of Fraud Detection Technology. In *Insider Threats in Cyber Security* (pp. 73-84). https://doi.org/10.1007/978-1-4419-7133-3_4

Forough, J., & Momtazi, S. (2021). Ensemble of deep sequential models for credit card fraud detection. *Applied Soft Computing, 99*. https://doi.org/10.1016/j.asoc.2020.106883

Fursov, I., Kovtun, E., Rivera-Castro, R., Zaytsev, A., Khasyanov, R., Spindler, M., & Burnaev, E. (2022). Sequence Embeddings Help Detect Insurance Fraud. *IEEE Access, 10*, 32060-32074. https://doi.org/10.1109/access.2022.3149480

Goecks, L. S., Korzenowski, A. L., Gonçalves Terra Neto, P., de Souza, D. L., & Mareth, T. (2022). Anti-money laundering and financial fraud detection: A systematic literature review. *Intelligent Systems in Accounting, Finance and Management, 29*(2), 71-85. https://doi.org/10.1002/isaf.1509

Gomes, C., Jin, Z., & Yang, H. (2021). Insurance fraud detection with unsupervised deep learning. *Journal of Risk and Insurance, 88*(3), 591-624. https://doi.org/10.1111/jori.12359

Grossi, M., Ibrahim, N., Radescu, V., Loredo, R., Voigt, K., von Altrock, C., & Rudnik, A. (2022). Mixed Quantum–Classical Method for Fraud Detection With Quantum Feature Selection. *IEEE Transactions on Quantum Engineering, 3*, 1-12. https://doi.org/10.1109/tqe.2022.3213474

Hashemi, S. K., Mirtaheri, S. L., & Greco, S. (2023). Fraud Detection in Banking Data by Machine Learning Techniques. *IEEE Access, 11*, 3034-3043. https://doi.org/10.1109/access.2022.3232287

Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances. *Expert Systems with Applications, 193*. https://doi.org/10.1016/j.eswa.2021.116429

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

Jullum, M., Løland, A., Huseby, R. B., Ånonsen, G., & Lorentzen, J. (2020). Detecting money laundering transactions with machine learning. *Journal of Money Laundering Control, 23*(1), 173-186. https://doi.org/10.1108/jmlc-07-2019-0055

Kalid, S. N., Ng, K.-H., Tong, G.-K., & Khor, K.-C. (2020). A Multiple Classifiers System for Anomaly Detection in Credit Card Data With Unbalanced and Overlapped Classes. *IEEE Access, 8*, 28210-28221. https://doi.org/10.1109/access.2020.2972009

Kapadiya, K., Patel, U., Gupta, R., Alshehri, M. D., Tanwar, S., Sharma, G., & Bokoro, P. N. (2022). Blockchain and AI-Empowered Healthcare Insurance Fraud Detection: an Analysis, Architecture, and Future Prospects. *IEEE Access, 10*, 79606-79627. https://doi.org/10.1109/access.2022.3194569

Karadayi, Y., Aydin, M. N., & Ogrenci, A. S. (2020). Unsupervised Anomaly Detection in Multivariate Spatio-Temporal Data Using Deep Learning: Early Detection of COVID-19 Outbreak in Italy. *IEEE Access, 8*, 164155-164177. https://doi.org/10.1109/access.2020.3022366

Kolli, C. S., & Tatavarthi, U. D. (2020). Fraud detection in bank transaction with wrapper model and Harris water optimization-based deep recurrent neural network. *Kybernetes, 50*(6), 1731-1750. https://doi.org/10.1108/k-04-2020-0239

Koreff, J., Weisner, M., & Sutton, S. G. (2021). Data analytics (ab) use in healthcare fraud audits. *International Journal of Accounting Information Systems, 42*. https://doi.org/10.1016/j.accinf.2021.100523

Lebichot, B., Verhelst, T., Le Borgne, Y.-A., He-Guelton, L., Oble, F., & Bontempi, G. (2021). Transfer Learning Strategies for Credit Card Fraud Detection. *IEEE Access, 9*, 114754-114766. https://doi.org/10.1109/access.2021.3104472

Lee, J., & Cho, S. (2021, Nov). Abuse detection in healthcare insurance with disease-treatment network embedding. *J Biomed Inform, 123*, 103936. https://doi.org/10.1016/j.jbi.2021.103936

Li, Z., Huang, M., Liu, G., & Jiang, C. (2021). A hybrid method with dynamic weighted entropy for handling the problem of class imbalance with overlap in credit card fraud detection. *Expert Systems with Applications, 175*. https://doi.org/10.1016/j.eswa.2021.114750

Lokanan, M. E., & Sharma, K. (2022). Fraud prediction using machine learning: The case of investment advisors in Canada. *Machine Learning with Applications, 8*. https://doi.org/10.1016/j.mlwa.2022.100269

Lucas, Y., Portier, P.-E., Laporte, L., He-Guelton, L., Caelen, O., Granitzer, M., & Calabretto, S. (2020). Towards automated feature engineering for credit card fraud detection using multi-perspective HMMs. *Future Generation Computer Systems, 102*, 393-402. https://doi.org/10.1016/j.future.2019.08.029

Mao, X. H. S. X. Z. J. L. (2021). Financial fraud detection using the related-party transaction knowledge graph. *Procedia Computer Science 199 (2022) 733–740*. https://doi.org/https://doi.org/10.1016/j.procs.2022.01.091

Matloob, I., Khan, S. A., & Rahman, H. U. (2020). Sequence Mining and Prediction-Based Healthcare Fraud Detection Methodology. *IEEE Access, 8*, 143256-143273. https://doi.org/10.1109/access.2020.3013962

Nguyen, N., Duong, T., Chau, T., Nguyen, V.-H., Trinh, T., Tran, D., & Ho, T. (2022). A Proposed Model for Card Fraud Detection Based on CatBoost and Deep Neural Network. *IEEE Access, 10*, 96852-96861. https://doi.org/10.1109/access.2022.3205416

Olowookere, T. A., & Adewale, O. S. (2020). A framework for detecting credit card fraud with cost-sensitive meta-learning ensemble approach. *Scientific African, 8*. https://doi.org/10.1016/j.sciaf.2020.e00464

Omair, B., & Alturki, A. (2020). A Systematic Literature Review of Fraud Detection Metrics in Business Processes. *IEEE Access, 8*, 26893-26903. https://doi.org/10.1109/access.2020.2971604

Patrick Laurent, T. C., Elsa Herzberg. (2015). Intelligent automation entering the business world.

Pourhabibi, T., Ong, K.-L., Kam, B. H., & Boo, Y. L. (2020). Fraud detection: A systematic literature review of graph-based anomaly detection approaches. *Decision Support Systems, 133*. https://doi.org/10.1016/j.dss.2020.113303

Pranto, T. H., Hasib, K. T. A. M., Rahman, T., Haque, A. B., Islam, A. K. M. N., & Rahman, R. M. (2022). Blockchain and Machine Learning for Fraud Detection: A Privacy-Preserving and Adaptive Incentive Based Approach. *IEEE Access, 10*, 87115-87134. https://doi.org/10.1109/access.2022.3198956

Rai, A. K. K. D., Rajendra (2020). Fraud Detection in Credit Card Data using Unsupervised Machine Learning Based Scheme. *Proceedings of the International Conference on Electronics and Sustainable Communication Systems (ICESC 2020)*. https://doi.org/10.1109/ICESC48915.2020.9155615

Rocha-Salazar, J.-d.-J., Segovia-Vargas, M.-J., & Camacho-Miñano, M.-d.-M. (2022). Detection of shell companies in financial institutions using dynamic social network. *Expert Systems with Applications, 207*. https://doi.org/10.1016/j.eswa.2022.117981

Rodrigues, V. F., Policarpo, L. M., da Silveira, D. E., da Rosa Righi, R., da Costa, C. A., Barbosa, J. L. V., Antunes, R. S., Scorsatto, R., & Arcot, T. (2022, 2022/11/01/). Fraud detection and prevention in e-commerce: A systematic literature review. *Electronic Commerce Research and Applications, 56*, 101207. https://doi.org/https://doi.org/10.1016/j.elerap.2022.101207

Sahni, S., Mittal, A., Kidwai, F., Tiwari, A., & Khandelwal, K. (2020). InsuranceFraudIdentificationusingComputerVisionandIoT:A Study of Field Fires. *International Conference on Smart Sustainable Intelligent Computing and Applications under ICITETM2020*. https://doi.org/https://doi.org/10.1016/j.procs.2020.06.008

Sánchez-Aguayo, M., Urquiza-Aguiar, L., & Estrada-Jiménez, J. (2021). Fraud Detection Using the Fraud Triangle Theory and Data Mining Techniques: A Literature Review. *Computers, 10*(10). https://doi.org/10.3390/computers10100121

Seify, M., Sepehri, M., Hosseinian-far, A., & Darvish, A. (2022, 2022/01/01/). Fraud Detection in Supply Chain with Machine Learning. *IFAC-PapersOnLine, 55*(10), 406-411. https://doi.org/https://doi.org/10.1016/j.ifacol.2022.09.427

Severino, M. K., & Peng, Y. (2021). Machine learning algorithms for fraud prediction in property insurance: Empirical evidence using real-world microdata. *Machine Learning with Applications, 5*. https://doi.org/10.1016/j.mlwa.2021.100074

Song, J., Qu, X., Hu, Z., Li, Z., Gao, J., & Zhang, J. (2021). A subgraph-based knowledge reasoning method for collective fraud detection in E-commerce. *Neurocomputing, 461*, 587-597. https://doi.org/10.1016/j.neucom.2021.03.134

Song, Z. (2020). *A Data Mining Based Fraud Detection Hybrid Algorithm in E-bank* 2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE),

Taha, A. A., & Malebary, S. J. (2020). An Intelligent Approach to Credit Card Fraud Detection Using an Optimized Light Gradient Boosting Machine. *IEEE Access, 8*, 25579-25587. https://doi.org/10.1109/access.2020.2971354

Takefuji, Y. (2023). Case report on enormous economic losses caused by fraud from Japan to the world. *Journal of Economic Criminology, 1*. https://doi.org/10.1016/j.jeconc.2023.100003

Thaifur, A., Maidin, M. A., Sidin, A. I., & Razak, A. (2021). How to detect healthcare fraud? "A systematic review". *Gac Sanit, 35 Suppl 2*, S441-S449. https://doi.org/10.1016/j.gaceta.2021.07.022

Tingfei, H., Guangquan, C., & Kuihua, H. (2020). Using Variational Auto Encoding in Credit Card Fraud Detection. *IEEE Access, 8*, 149841-149853. https://doi.org/10.1109/access.2020.3015600

Vanhoeyveld, J., Martens, D., & Peeters, B. (2020). Value-added tax fraud detection with scalable anomaly detection techniques. *Applied Soft Computing, 86*. https://doi.org/10.1016/j.asoc.2019.105895

Vaughan, G. (2020). Efficient big data model selection with applications to fraud detection. *International Journal of Forecasting, 36*(3), 1116-1127. https://doi.org/10.1016/j.ijforecast.2018.03.002

Wang, H., Wang, W., Liu, Y., & Alidaee, B. (2022). Integrating Machine Learning Algorithms With Quantum Annealing Solvers for Online Fraud Detection. *IEEE Access, 10*, 75908-75917. https://doi.org/10.1109/access.2022.3190897

Westland, J. C. (2022). A comparative study of frequentist vs Bayesian A/B testing in the detection of E-commerce fraud. *Journal of Electronic Business & Digital Economics, 1*(1/2), 3-23. https://doi.org/10.1108/jebde-07-2022-0020

Wu, Y., Xu, Y., & Li, J. (2021). Fraudulent traffic detection in online advertising with bipartite graph propagation algorithm. *Expert Systems with Applications, 185*. https://doi.org/10.1016/j.eswa.2021.115573

Xia, H., Ma, H., & Cheng, P. (2021). PE-EDD: An efficient peer-effect-based financial fraud detection approach in publicly traded China firms. *CAAI Transactions on Intelligence Technology, 7*(3), 469-480. https://doi.org/10.1049/cit2.12057

Xiuguo, W., & Shengyong, D. (2022). An Analysis on Financial Statement Fraud Detection for Chinese Listed Companies Using Deep Learning. *IEEE Access, 10*, 22516-22532. https://doi.org/10.1109/access.2022.3153478

Yan, C., Li, Y., Liu, W., Li, M., Chen, J., & Wang, L. (2020). An artificial bee colony-based kernel ridge regression for automobile insurance fraud identification. *Neurocomputing, 393*, 115-125. https://doi.org/10.1016/j.neucom.2017.12.072

Zhang, X., Han, Y., Xu, W., & Wang, Q. (2021). HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture. *Information Sciences, 557*, 302-316. https://doi.org/10.1016/j.ins.2019.05.023

Zhou, H., Sun, G., Fu, S., Wang, L., Hu, J., & Gao, Y. (2021). Internet Financial Fraud Detection Based on a Distributed Big Data Approach With Node2vec. *IEEE Access, 9*, 43378-43386. https://doi.org/10.1109/access.2021.3062467

Zhou, S., He, J., Yang, H., Chen, D., & Zhang, R. (2020). Big Data-Driven Abnormal Behavior Detection in Healthcare Based on Association Rules. *IEEE Access, 8*, 129002-129011. https://doi.org/10.1109/access.2020.3009006

Zhu, H., Liu, G., Zhou, M., Xie, Y., Abusorrah, A., & Kang, Q. (2020). Optimizing Weighted Extreme Learning Machines for imbalanced classification and application to credit card fraud detection. *Neurocomputing, 407*, 50-62. https://doi.org/10.1016/j.neucom.2020.04.078

Zhu, X., Ao, X., Qin, Z., Chang, Y., Liu, Y., He, Q., & Li, J. (2021, Nov 28). Intelligent financial fraud detection practices in post-pandemic era. *Innovation (Camb), 2*(4), 100176. https://doi.org/10.1016/j.xinn.2021.100176