Jurnal Bina Akuntansi
Volume 13, Number 1, 2026 pp. 41-60
ISSN: 2338-1132 E-ISSN : 2656-9515
Open Access: https://jurnal.wym.ac.id/JBA

MACHINE LEARNING TECHNIQUES IN DETECTING FRAUD: A STATE OF THE ART REVIEW IN THE SCOPUS DATABASE

Juli Riyanto Tri Wijaya[1*], Dien Noviany Rahmatika[2], Eliada Herwiyanti[3]
[1] juli.wijaya@upstegal.ac.id, Fakultas Ekonomi dan Bisnis, Universitas Pancasakti Tegal, Indonesia
[2] diennovi@upstegal.ac.id, Fakultas Ekonomi dan Bisnis, Universitas Pancasakti Tegal, Indonesia
[3] eliada.herwiyanti@unsoed.ac.id, Fakultas Ekonomi dan Bisnis, Universitas Jenderal Soedirman, Indonesia

INFO ARTIKEL
Riwayat Artikel:
Pengajuan : 04/08/2025
Revisi : 18/12/2025
Penerimaan : 05/01/2026

Kata Kunci:
Pembelajaran Mesin, Penipuan, Deteksi Penipuan, AI, Tinjauan Literatur

Keywords:
Machine Learning, Fraud, Fraud Detection, Explainable AI, Systematic Literature Review

DOI:
10.52859/jba.v13i1.825

A B S T R A K

Penelitian ini memetakan perkembangan dan dampak penggunaan *machine learning* (ML) untuk deteksi penipuan melalui tinjauan 106 artikel terindeks Scopus yang terbit pada 2009–2025 di bidang Bisnis, Manajemen, Akuntansi, Ekonomi, dan Keuangan. Tren publikasi meningkat tajam dengan lonjakan setelah 2020. Dibanding metode tradisional, ML umumnya memberikan deteksi yang lebih cepat dan lebih akurat. Meski demikian, adopsi praktis masih terhambat oleh rendahnya interpretabilitas (model *black box*), ketidakseimbangan kelas data, keterbatasan generalisasi lintas konteks, serta minimnya implementasi dan evaluasi berbasis data operasional nyata. Literatur juga terfragmentasi lintas disiplin dan belum memiliki standar evaluasi yang seragam. Studi ini merekomendasikan kolaborasi antarbidang, penguatan *explainable* AI, akses dataset realistis, serta tata kelola etika agar sistem deteksi penipuan lebih andal, transparan, dan mudah diterapkan serta diskalakan. Implikasinya mendukung peneliti, auditor, dan regulator dalam merancang kebijakan berbasis data.

A B S T R A C T

This study reviews 106 Scopus-indexed articles (2009–2025) in Business, Management, Accounting, Economics, and Finance to map how machine learning (ML) has evolved and what it implies for fraud detection. Publication volume increases sharply, especially after 2020. Compared with traditional approaches, ML generally offers faster and more accurate identification. Yet broad adoption is constrained by limited interpretability (black-box models), severe class imbalance, weak cross-context generalizability, and scarce deployments evaluated on real operational data. The evidence base is also fragmented across disciplines and lacks consistent benchmarking and reporting practices. We propose stronger interdisciplinary collaboration, wider use of explainable AI, access to realistic shared datasets, and ethics-by-design governance to improve transparency, robustness, and scalability. These insights help researchers, auditors, and regulators prioritize actionable research and guide practical implementation across diverse organizational settings worldwide.

Introduction

The exponential growth of digital transactions and the increasing complexity of business operations have made fraud one of the most critical and persistent threats facing modern financial systems. Traditional rule-based approaches to fraud detection, while effective in well-defined scenarios, often struggle to cope with the evolving and adaptive nature of fraudulent behavior. This challenge has prompted the integration of more dynamic and intelligent systems, particularly those driven by machine learning (ML), to enhance the ability of organizations to detect fraud in real-time and with greater accuracy. Over the past two decades, ML has emerged as a powerful set of tools capable of identifying complex, nonlinear patterns in large datasets, enabling systems to learn from past behaviors and improve detection capabilities without explicit programming. As a result, researchers and practitioners alike have turned to machine learning to revolutionize the landscape of fraud detection (Wang & Xu, 2018).

Machine learning encompasses a broad spectrum of techniques, including supervised learning, unsupervised learning, and reinforcement learning, each offering unique advantages for different fraud detection contexts. Supervised methods such as decision trees, support vector machines (SVM), logistic

* Penulis Korespondensi: Juli Riyanto Tri Wijaya / juli.wijaya@upstegal.ac.id

regression, and neural networks have been widely utilized for classifying transactions as fraudulent or legitimate based on labeled historical data (Galiautdinov, 2023; Ding *et al*., 2025). Unsupervised learning approaches, including clustering and anomaly detection techniques, are often applied when labeled data is unavailable, relying on pattern deviations to flag suspicious activity (Bao *et al*., 2021; Shi & Zhao, 2023). More recently, hybrid and ensemble models that combine multiple learning paradigms have been explored to improve robustness and detection rates across different datasets (Mirhashemi *et al*., 2023; Papík & Papíková, 2022).

Numerous empirical studies have confirmed the superior performance of machine learning models over conventional statistical methods. Demonstrated that neural networks and decision trees significantly outperform logistic regression in identifying fraudulent financial statements. Similarly, Appavu (2025) highlighted the utility of convolutional neural networks (CNNs) in detecting subtle fraud patterns in unstructured data sources. The deployment of ML algorithms in real-world settings, such as banking fraud prevention systems, credit card fraud detection, insurance claim assessments, and corporate auditing, has reinforced their practical viability and economic relevance (Kini *et al*., 2022; Kolodiziev *et al*., 2020; Vandervorst *et al*., 2022). However, despite these advances, several methodological and practical issues remain unresolved, including the handling of class imbalance, data privacy concerns, computational complexity, and the interpretability of complex models (Subramaniam *et al*., 2024; Zhao *et al*., 2025).

The machine learning (ML) literature on fraud detection is substantial and growing, but it remains fragmented across disciplines and application domains. Aiemsuwan & Srikamdee (2024) stress that, despite advances in algorithms, standardized frameworks for evaluating and comparing ML techniques are still lacking, while Lin *et al.* (2024) argue that heterogeneous data sources, model settings, and metrics hinder generalizability and reproducibility. These limitations make a structured synthesis necessary to map the state of the art, identify trends and gaps, and guide future research (Ghosh *et al*., 2023; Mishra *et al*., 2022); therefore, this study reviews Scopus-indexed articles to trace the evolution of ML in fraud detection, compare methods using common metrics, highlight emerging directions and unresolved challenges, and provide recommendations for research and practical implementation.

One notable development in fraud detection is the growing integration of deep learning and advanced neural architectures. Techniques such as long short-term memory (LSTM) networks are increasingly adopted to capture sequential and temporal behaviors in transactions, while generative adversarial networks (GANs) are explored to generate synthetic fraud samples and help mitigate class-imbalance problems (Qiu & Luo, 2024; Zhai *et al*., 2017). These models show promise in learning complex time-dependent signals and rare-event patterns that frequently characterize fraud. However, their practical use also raises concerns regarding high computational requirements and limited transparency in model decision-making, which can complicate regulatory compliance and real-world deployment. Consequently, the development of explainable AI (XAI) has become essential to ensure that model outputs can be interpreted and trusted by auditors and organizational decision-makers (Zkik *et al*., 2024; Pandey, 2024).

In parallel, the increasing availability of real-time transaction streams and streaming analytics introduces new opportunities and additional complexity for ML-based fraud detection. Real-time detection demands models that can process high-velocity data and adapt quickly to emerging fraud strategies without requiring frequent retraining from scratch (Hoseini *et al*., 2021; Zhai *et al*., 2017). This requirement drives the need for scalable, low-latency ML frameworks capable of operating in distributed environments while maintaining strong detection performance, particularly in mobile payments and

digital banking, where speed and accuracy are critical. Yet, implementation remains challenging, as system stability, false-positive costs, and model drift continue to be central concerns in both research and industry practice (Papík & Papíková, 2022; Zhao *et al*., 2025). Overall, the adoption of ML represents a major paradigm shift in fraud detection, but sustained progress still depends on more deployment-aware, ethical, and explainable solutions supported by rigorous and consistent evaluation.

Several recent studies have advanced the application of machine learning (ML) in fraud detection, yet notable research gaps remain. Detthamrong *et al.* (2024) proposed an ensemble framework combining decision trees and boosting algorithms, which demonstrated high accuracy in financial fraud detection. However, their study was limited to structured tabular data, leaving out unstructured data and multimodal contexts. Gadde *et al.* (2024) introduced a deep learning model using attention-based mechanisms for credit card fraud detection. While the model achieved superior performance over traditional neural networks, its reliance on synthetic data generation methods like SMOTE raised concerns about model generalizability in real-world scenarios.

Hamisu and Mansour (2021) investigated the role of feature engineering in improving ML performance in insurance fraud detection. Their work emphasized domain knowledge integration but lacked comparative evaluation across different algorithm types. Similarly, Li *et al.* (2025) proposed a real-time fraud detection model using LSTM networks, yet their research focused narrowly on temporal data and omitted the issue of model explainability. Together, these studies reflect fragmented progress, focusing on specific data types, model types, or domains, which highlights the need for a comprehensive, cross-domain synthesis of empirical findings. This gap underpins the relevance of conducting a systematic, Scopus-based state-of-the-art review. This study aims to comprehensively examine the development and impact of machine learning techniques in the domain of fraud detection through an in-depth empirical literature review.

Literature Review

The application of machine learning (ML) in fraud detection has gained momentum across finance, auditing, banking, and e-commerce. Researchers have explored various ML methods, from classical to deep learning approaches. Aboelfotoh *et al.* (2025) demonstrated the effectiveness of ensemble models in banking fraud detection, though noted limitations in model portability. Similarly, Banerjee and Menon (2019) highlighted the need for context-aware models to improve cross-sector reliability. Deep learning has become a leading trend. Gupta and Mehta (2024) applied convolutional neural networks for accounting fraud detection with strong performance, though lacking model explainability. Knuth and Ahrholdt (2022) echoed this concern, stressing the need for interpretability in financial AI. El Hlouli *et al.* (2023) explored graph neural networks for transaction fraud detection, but their work was limited to specific datasets.

Several studies address data-related challenges. Bao *et al.* (2022) and Lu *et al.* (2022) tackled class imbalance using synthetic data and undersampling, which may compromise data realism. The Erratum to: Detecting Accounting Fraud... (2022) underlined the importance of high-quality empirical data, correcting earlier issues with labeling and sample bias. Hybrid and ensemble models have been proposed to boost accuracy and resilience. Lata Jeyaraj *et al.* (2024) used decision trees with gradient boosting for e-commerce fraud, while Hudnurkar *et al.* (2024) combined hybrid feature selection with random forests in insurance fraud detection. Tayebi and El Kafhali (2025) introduced a real-time fraud detection model via federated learning, addressing latency and privacy, though interpretability remains a challenge.

Other studies focus on behavioral and contextual factors. Ibrahim and Badr (2025) designed models sensitive to user behavior drift, while Sharma and Pandey (2023) used unsupervised learning to detect anomalies in banking transactions. Jaidhan *et al*. (2019) and Vičič & Tošić (2022) explored clustering and semi-supervised learning but faced reproducibility and benchmarking issues. In summary, although ML-based fraud detection research has advanced significantly, the literature remains fragmented across domains, algorithms, and evaluation metrics. There is a lack of standardized benchmarks, cross-dataset validations, and comparative studies. These gaps highlight the need for a comprehensive Scopus-based review to map current approaches, assess their effectiveness, and guide future research and practical implementation.

While prior reviews on fraud research often provide broad mappings of fraud topics or summarize algorithmic options at a high level, this review makes the academic contribution more explicit by offering an updated, finance-oriented synthesis of machine learning–based fraud detection with an emphasis on methodological rigor and research gaps that affect real-world validity. Specifically, our review is novel in three ways. First, it consolidates 106 Scopus-indexed journal articles (2009–2025) within the subject areas of Business, Management and Accounting, and Economics, Econometrics and Finance, thereby capturing evidence that is directly relevant to financial decision-making, governance, and managerial implications—areas that are sometimes underrepresented in technically oriented reviews. Second, beyond listing models, we develop a structured synthesis that links (i) ML approach families (supervised/unsupervised/hybrid/deep learning), (ii) fraud contexts and institutional settings, and (iii) evaluation practices (metrics, imbalance handling, validation design), enabling cross-study comparison and revealing where performance claims are not fully comparable. Third, we contribute a critical assessment of recurring methodological limitations (e.g., class imbalance treatment, temporal generalizability, leakage risks, and limited reproducibility) and translate these into a clear research agenda (time-aware validation, cost-sensitive evaluation, explainable/auditable ML, and deployment-aware workflows). Collectively, these contributions clarify what is genuinely known, what remains uncertain, and which directions are most promising for advancing fraud detection research in finance and management.

Method

This study employs a Systematic Literature Review (SLR) to identify, evaluate, and synthesize scholarly evidence on the application of machine learning (ML) for fraud detection. The literature search was conducted in the Scopus database due to its broad coverage of peer-reviewed journals and the availability of structured bibliographic metadata. The search scope covered publications from 2009–2025 and targeted records indexed through the Title, Abstract, and Keywords fields. The advanced search query used was: TITLE-ABS-KEY(("machine learning" OR "deep learning") AND ("fraud detection" OR fraud) AND (detect OR classif OR identif*))**. To ensure disciplinary relevance, results were limited to the subject areas Business, Management and Accounting, and Economics, Econometrics and Finance, with additional filters applied for document type (journal article), language (English), and publication stage (final).

Study selection followed a transparent multi-stage screening procedure. First, all retrieved records were exported, and duplicates were removed. Second, a title and abstract screening was performed to retain only studies clearly aligned with ML-based fraud detection. Third, the remaining papers underwent full-text eligibility assessment to confirm that each article met the predefined criteria and provided sufficient methodological detail for synthesis. Articles were included if they were Scopus-indexed journal

articles published between 2009 and 2025, explicitly investigated ML approaches (including deep learning and hybrid models) for fraud detection, and reported essential information such as model/approach description, dataset characteristics, and evaluation metrics. Articles were excluded if they were not journal articles (e.g., conference proceedings, book chapters, editorials), did not clearly involve ML, addressed generic anomaly detection without a fraud-detection objective, were duplicates, or lacked adequate methodological reporting. Following this process, 106 articles were retained as the final review corpus.

After eligibility confirmation, a lightweight quality appraisal was applied to ensure that the included studies reported key elements (clarity of objectives, dataset description, ML method specification, and evaluation procedures). Data were then extracted using a structured coding form capturing: ML technique category (supervised, unsupervised, hybrid, deep learning), application domain (e.g., banking, insurance, e-commerce, auditing), data issues (e.g., class imbalance, real-world vs. synthetic data), and performance measures (accuracy, precision, recall, F1-score, AUC-ROC), as well as limitations and research gaps. Finally, the synthesis combined descriptive/bibliometric profiling (e.g., publication trends and affiliation patterns based on Scopus metadata) with thematic analysis to compare recurring methods, challenges, evaluation practices, and emerging directions in ML-based fraud detection research.

Result and Discussion

Result

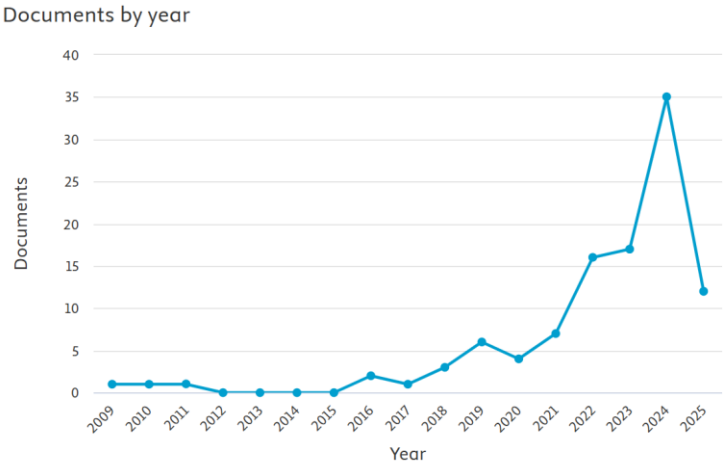

Figure 1. Documents by year

Source: Processed by Researchers (2025)

Figure 1. Illustrates the distribution of published research articles related to the use of machine learning in fraud detection from 2009 to 2025. The data reveal a gradual increase in scholarly attention over the years, with a particularly sharp rise beginning in 2020. From 2009 to 2016, publication numbers remained relatively flat, averaging fewer than 5 documents per year, indicating limited exploration of this topic during the early stages. A modest uptick began in 2017, with incremental growth through 2020, reflecting a rising awareness of the potential of machine learning in addressing fraud. A noticeable acceleration occurred from 2021 onwards, with publications increasing significantly, nearly doubling each year, culminating in a peak in 2024 with over 35 documents published. This peak suggests a surge of interest, likely driven by advancements in AI technologies, the increasing frequency of digital fraud, and the growing demand for data-driven decision-making in financial systems. However, the sharp

decline in 2025 may be attributed to the partial data availability for that year, as it may not yet be complete. Overall, the trend underscores a growing research momentum in recent years, validating the relevance and timeliness of conducting a comprehensive literature review on machine learning applications in fraud detection.

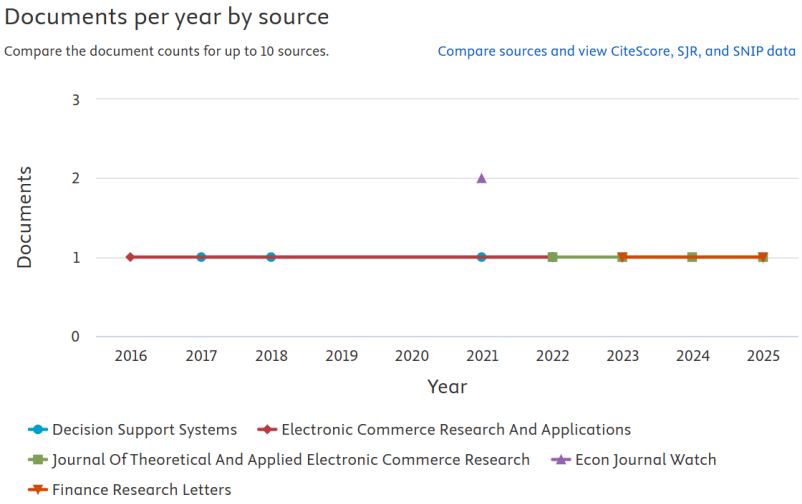

Figure 2. Documents per year by source

Source: Processed by Researchers (2025)

Figure 2. Illustrates the distribution of published articles on machine learning in fraud detection across various journals from 2016 to 2025. Most journals contribute only one or two papers per year, reflecting a relatively even but limited spread. Decision Support Systems and Electronic Commerce Research and Applications appear as consistent contributors, especially in 2016, 2018, and 2020. Notably, Econ Journal Watch published two articles in 2020, the only instance of multiple publications by a single journal in one year. Other journals, such as Journal of Theoretical and Applied Electronic Commerce Research and Finance Research Letters, show sporadic contributions mostly between 2021 and 2025. This pattern suggests that while interest in fraud detection using machine learning is increasing, it remains a developing focus within individual journals. The variety of sources from finance to information systems emphasizes the interdisciplinary nature of the field. The absence of a dominant journal highlights the fragmented state of current research and signals the need for more centralized publication efforts, such as special issues or dedicated journals. These findings further justify the relevance of conducting a comprehensive literature review to integrate dispersed insights into a unified body of knowledge.

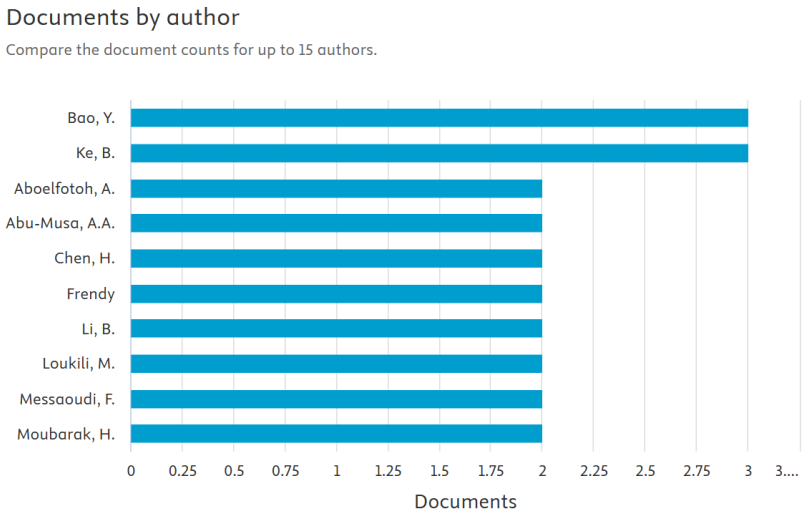

Figure 3. Documents per year by author

Source: Processed by Researchers (2025)

Figure 3 compares the top 10 most prolific authors in machine learning applications for fraud detection. Bao, Y. and Ke, B. lead with three publications each, followed by eight authors, including Aboelfotoh, H., Abu-Musa, A.A., and Chen, H. with two publications each. The relatively even distribution of contributions suggests that the field is supported by a diverse group of researchers, rather than being dominated by a single individual or institution. This diversity reflects the interdisciplinary nature of fraud detection research, spanning finance, computer science, and management. Although publication counts remain modest, the presence of recurring contributors indicates an emerging core community. This offers opportunities for collaboration and highlights the need for stronger research networks and methodological standards. Overall, the authorship pattern supports the importance of a structured literature review to integrate and assess contributions from these key researchers within broader academic trends.

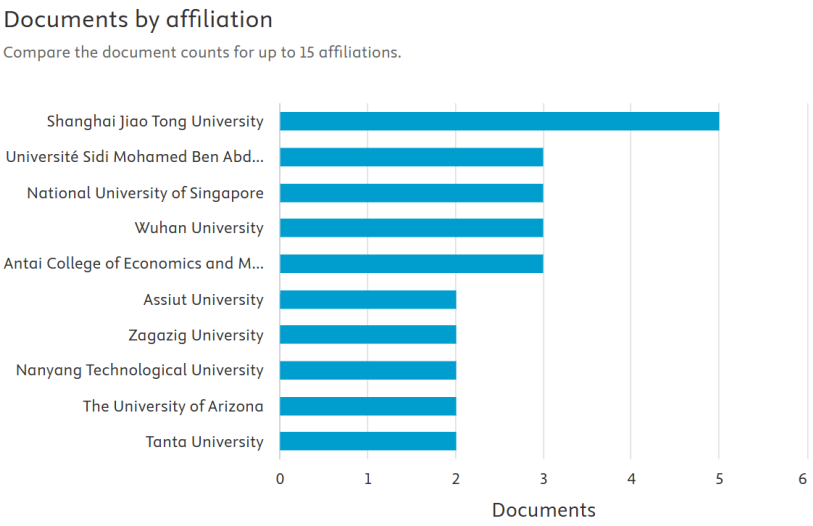

Figure 4. Documents by affiliation

Source: Processed by Researchers (2025)

Figure 4 shows the number of publications on machine learning in fraud detection by academic institutions. Shanghai Jiao Tong University leads with five publications, highlighting its strong focus in this area. Other notable contributors include Université Sidi Mohamed Ben Abdellah, National University

of Singapore, Wuhan University, and Antai College, each with three publications. Institutions such as Assiut University, Nanyang Technological University, and the University of Arizona follow with two. This distribution reflects growing global interest across Asia, Africa, and North America, yet also shows that contributions are concentrated among a few universities. While the field is gaining traction, the relatively low output per institution indicates a need for greater investment and collaboration. The findings emphasize the importance of expanding cross-institutional and international partnerships to strengthen research capacity and innovation in fraud detection using machine learning.

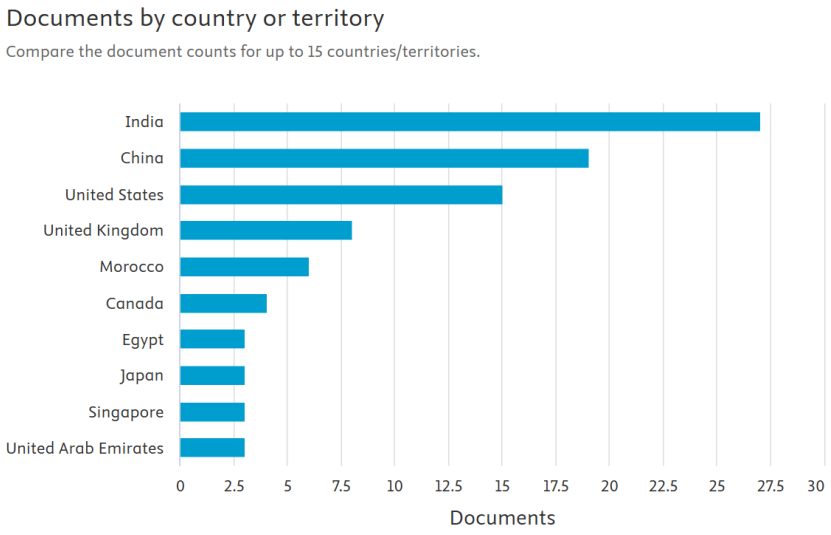

Figure 5. Documents by country or territory

Source: Processed by Researchers (2025)

Figure 5 illustrates the country-wise distribution of research on machine learning in fraud detection. India leads with nearly 30 publications, likely driven by rapid digitalization and rising fraud cases. China follows with just under 20, reflecting strong AI research investment, while the U.S. ranks third with 15 documents, showing continued engagement from North America. The UK, Morocco, Canada, and Egypt contribute moderately, indicating growing global interest, including from developing regions. Countries like Japan, Singapore, and the UAE also show emerging activity. While the data confirms fraud detection as a globally relevant topic, it also reveals disparities in research output, suggesting the need for broader international collaboration and support for underrepresented countries. This uneven distribution underscores the importance of inclusive, cross-border efforts to advance machine learning applications in fraud detection.

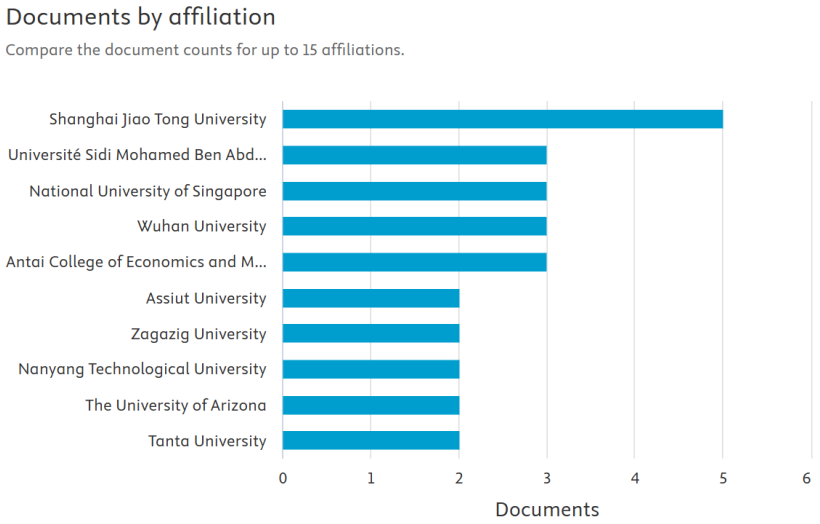

Figure 6. Documents by affiliation

Source: Processed by Researchers (2025)

Figure 6 shows the distribution of research publications on machine learning in fraud detection by academic institutions. Shanghai Jiao Tong University leads with five publications, followed by institutions like Université Sidi Mohamed Ben Abdellah, National University of Singapore, and Wuhan University with three each. Contributions come from a diverse set of universities across Asia, Africa, and the Middle East, highlighting the global and interdisciplinary nature of the field. While no single institution dominates, the growing number of contributors reflects a decentralized yet expanding research community. The relatively low output per institution suggests that the field is still emerging, with opportunities for increased collaboration, funding, and focused research efforts. Overall, the data indicates a promising trend of international academic engagement and the need for stronger institutional networks to advance innovation in fraud detection using machine learning.

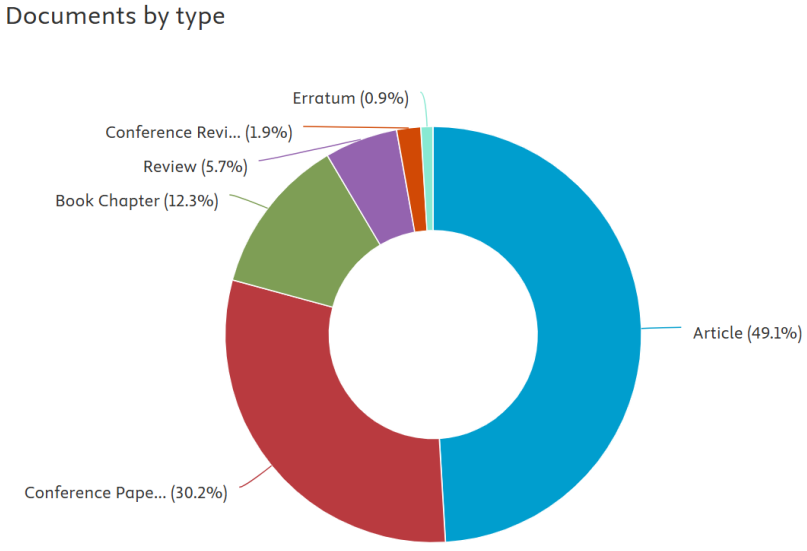

Figure 7. Documents by type

Source: Processed by Researchers (2025)

Figure 7 presents the types of documents in the literature on machine learning in fraud detection. Journal articles make up the largest share at 49.1%, indicating a strong foundation of peer-reviewed, theory-based research. Conference papers follow at 30.2%, reflecting the field's evolving and

experimental nature. Book chapters (12.3%) show contributions from multidisciplinary perspectives, while reviews (5.7%) suggest limited efforts to synthesize existing knowledge. Conference reviews (1.9%) and errata (0.9%) are minimal. Overall, the mix of document types highlights both academic maturity and technological progress in the field. However, the relatively low number of review papers points to the need for more systematic literature studies to unify findings and guide future research. The diversity of formats also reflects the interdisciplinary and globally collaborative nature of fraud detection research using machine learning.

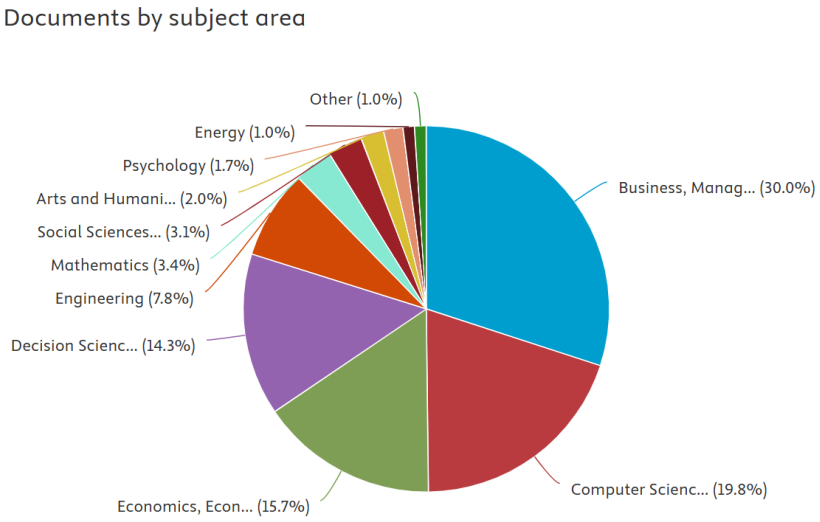

Figure 8. Documents by subject area

Source: Processed by Researchers (2025)

Figure 8 shows the multidisciplinary spread of research on machine learning in fraud detection. Most publications fall under Business, Management, and Accounting (30%), highlighting the focus on organizational and financial fraud. Computer Science follows at 19.8%, emphasizing the role of algorithms and data processing. Economics and Finance (15.7%) and Decision Sciences (14.3%) reflect interest in financial systems and risk modeling. Engineering (7.8%) and Mathematics (3.4%) contribute to the technical foundation, while Social Sciences, Arts and Humanities, and Psychology offer emerging behavioral and ethical insights. Smaller shares from Energy and interdisciplinary fields suggest broader interest. The data underscores the interdisciplinary nature of the field, combining technical rigor with practical relevance. However, lower contributions from social and psychological domains point to opportunities for deeper exploration of human and ethical aspects. This reinforces the need for a comprehensive, cross-disciplinary literature review to fully capture the complexity and future directions of ML-based fraud detection.

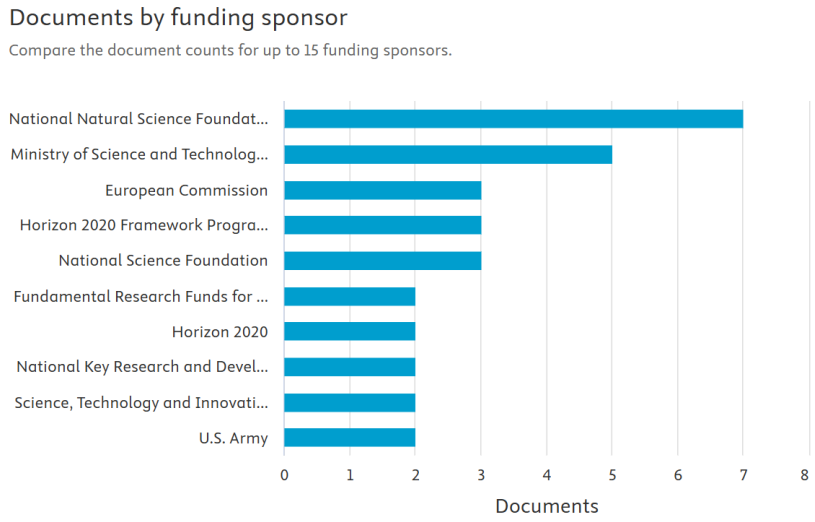

Figure 9. Documents by funding sponsor

Source: Processed by Researchers (2025)

Figure 9 shows the distribution of funding sources for research on machine learning in fraud detection. The National Natural Science Foundation leads with seven funded publications, followed by the Ministry of Science and Technology with five, highlighting strong government support—especially from China. International bodies like the European Commission, Horizon 2020, and the U.S. National Science Foundation each funded three documents, reflecting global interest in digital security. Other organizations, including the U.S. Army and various national programs, contributed to two publications each. While funding is primarily concentrated among a few key public agencies, this pattern underscores the strategic importance of fraud detection research. It also points to opportunities for broader investment, especially from the private sector. Overall, the data highlights the need for increased collaboration between governments, academia, and industry to scale innovation and ensure real-world impact of AI in combating fraud.

Discussion

The findings from this comprehensive review of 106 Scopus-indexed articles reveal an accelerating global interest in the application of machine learning (ML) to fraud detection, particularly from 2020 onwards. This temporal surge aligns with broader digital transformations and increasing instances of complex fraudulent behaviors that traditional systems struggle to detect effectively. The shift toward ML reflects its capacity for real-time learning, adaptive decision-making, and handling of large, heterogeneous datasets features essential for modern fraud detection.

The analysis also confirms the interdisciplinary nature of the field, with publications spanning subject areas such as business, management, computer science, and economics. Business and management account for the highest share (30%), underscoring the strategic and financial relevance of fraud prevention in corporate governance and operational efficiency. This is followed by computer science (19.8%) and economics (15.7%), highlighting the dual technical and financial complexity involved in designing fraud detection systems. Notably, decision sciences (14.3%) suggest a growing focus on optimization and analytics in detecting irregularities. As discussed by Banerjee and Menon (2019), the integration of stochastic treatments and advanced data modeling in decision-making frameworks has opened new frontiers in predictive fraud detection systems.

A key insight from the study is the dominance of supervised learning models, such as support vector machines (SVM), decision trees, and neural networks (Galiautdinov, 2023). These models perform well

when high-quality labeled data is available, offering strong classification capabilities. However, the limitations of supervised approaches especially their reliance on labeled datasets prompted the exploration of unsupervised and hybrid models. For example, Bao *et al.* (2022) and Shi & Zhao (2023) illustrate the promise of anomaly detection and clustering techniques in contexts where fraud patterns are not easily labeled in advance.

In terms of publication venues, the analysis reveals that no single journal dominates the research landscape. Rather, contributions are dispersed across journals like Decision Support Systems, Electronic Commerce Research and Applications, and Finance Research Letters. This fragmentation, while indicative of wide-ranging interest, also highlights a lack of centralized knowledge and a need for consolidation through literature reviews and meta-analyses (Gupta & Mehta, 2024).

The study's authorship and institutional affiliations underscore the global distribution of research expertise. India emerges as the leading contributor by country, with Shanghai Jiao Tong University as the top-affiliated institution. Such geographical diversity reflects the universal relevance of fraud detection challenges but also reveals a disparity in research intensity between countries. The concentration of funding in organizations such as the National Natural Science Foundation and the Ministry of Science and Technology further highlights the pivotal role of national investment in driving innovation (Chen & Zhai, 2023; Bao *et al*., 2022).

Document type distribution shows that nearly half of the literature comprises journal articles (49.1%), followed by conference papers (30.2%). The high number of conference papers indicates ongoing experimentation and the rapid evolution of the field. However, the relatively lower percentage of review papers (5.7%) highlights a gap in synthesis-oriented contributions that can unify fragmented research strands. This gap reinforces the need for systematic reviews such as this one, which draw connections across disparate findings and establish a holistic understanding of the field.

Despite growing adoption, several limitations persist in current research. One critical issue is the "black box" nature of deep learning models like CNNs and LSTMs, which lack interpretability (Knuth & Ahrholdt, 2022; Li *et al*., 2025). As financial and legal systems demand transparency, models must evolve to include explainable AI (XAI) mechanisms such as SHAP and LIME. Moreover, the challenge of class imbalance, where fraudulent instances are significantly rarer than legitimate ones, remains unresolved. While synthetic oversampling techniques like SMOTE Gadde *et al.* (2024) help mitigate this issue, they risk distorting the statistical integrity of datasets (Erratum, 2022).

Several studies have attempted to address these limitations through hybrid and ensemble models. For instance, Lata Jeyaraj *et al.* (2024) combined decision trees with gradient boosting in e-commerce contexts, achieving better generalization and robustness. Similarly, Hudnurkar *et al.* (2024) proposed hybrid feature selection with random forest classifiers, demonstrating improved classification accuracy in insurance fraud detection. Yet, the generalizability of these models across different fraud types and industries remains uncertain.

The increasing use of real-time and streaming data introduces additional complexities. As noted by Lu *et al.* (2022), the deployment of graph neural networks in real-time environments is promising but computationally demanding. Streaming models must account for data velocity, adapt to new fraud patterns, and minimize false positives, which can undermine user trust. Tayebi & El Kafhali (2025) addressed this challenge through federated learning and autoencoders, but scalability and deployment in real-world environments are still underexplored.

Behavioral modeling represents an emerging area of research. Ibrahim and Badr (2025) proposed behavior-sensitive AI models that adapt to changes in user activity over time. These models are

especially useful in identifying low-frequency, high-impact fraud types. Sharma & Pandey (2023) and Vičič & Tošić (2022) further highlighted the importance of incorporating behavioral analytics into fraud detection systems, moving beyond static pattern recognition.

Another key contribution from this review is the recognition of contextual fraud detection. As noted by El Hlouli *et al.* (2023), fraud in networked environments (e.g., blockchain, e-commerce) requires contextualized detection mechanisms such as stacked autoencoders and kernel ELMs optimized by evolutionary algorithms. These techniques reflect the increasing sophistication of fraudulent methods and the need for equally complex detection tools.

Although the reviewed studies (n = 106) consistently report that machine learning improves fraud detection performance, a closer inspection shows that the evidence is heterogeneous and not always comparable across domains, datasets, and evaluation settings. Many papers present strong headline metrics, yet the reported gains often depend on task framing, data availability, and validation design rather than on model superiority alone. Consequently, the central contribution of this review is not merely that ML "works" for fraud detection, but that the current literature reveals recurring methodological weaknesses and practical constraints that shape what these performance claims actually mean for real-world financial decision making.

A critical issue concerns data representativeness and class imbalance. Fraud datasets are naturally skewed, and while most studies acknowledge imbalance, mitigation strategies (e.g., SMOTE, undersampling, cost-sensitive learning) are applied inconsistently and sometimes without adequate justification. This matters because improvements in overall accuracy can be misleading when the fraud class is rare; small shifts in prevalence can change accuracy substantially without improving the detection of fraudulent cases. Therefore, studies that emphasize accuracy without reporting fraud-class recall/precision (or PR-AUC) may inadvertently overstate effectiveness. The review indicates that more credible evidence comes from papers that (1) explicitly optimize for minority-class performance, (2) use cost-sensitive objectives aligned with financial loss, and (3) provide robust sensitivity analyses under varying fraud prevalence.

Another recurring limitation is evaluation design and generalizability. Many studies rely on single-dataset experiments and report results from random train–test splits that may not reflect deployment realities (e.g., temporal drift, policy changes, evolving attacker strategies). In fraud detection, concept drift is expected; thus, random splitting risks inflating performance if patterns from future periods leak into training. More convincing designs use time-aware validation, rolling windows, or out-of-time testing, yet these remain less common. As a result, the literature currently provides limited certainty about how well proposed models generalize across time, institutions, and transaction contexts. This gap suggests that future work should treat temporal robustness and cross-domain transferability as primary performance criteria rather than optional extensions.

The review also highlights a tension between model complexity and operational constraints. Deep learning and hybrid models often demonstrate improvements, but the gains are not always large enough to justify higher computational costs, increased tuning burden, and reduced interpretability—especially in regulated financial settings where explanations are required for auditability and customer dispute resolution. Many papers still treat explainability as an afterthought, which is problematic because fraud detection decisions can trigger account freezes, investigations, or reputational harm. More practice-relevant studies are those that combine strong detection performance with transparent decision rationale (e.g., SHAP/LIME, rule extraction, monotonic constraints) and clearly discuss how explanations can be integrated into investigation workflows.

From a research synthesis perspective, the field would benefit from stronger standards for reproducibility and reporting. A substantial share of studies provide insufficient detail about preprocessing, feature engineering, hyperparameter tuning, threshold selection, and leakage control. This limits replication and creates uncertainty about whether reported improvements are attributable to the proposed method or to undocumented pipeline choices. To address this, the review suggests adopting a minimum reporting checklist for fraud-ML studies, including: dataset description and provenance, imbalance handling, leakage prevention strategy, validation protocol (preferably time-based), thresholding method, full metric set (including PR-AUC, recall/precision for fraud class), and ablation tests to isolate which components drive gains.

Finally, the evidence indicates that the most impactful future direction is not simply "more accurate models," but deployment-aware fraud analytics: models that remain robust under drift, handle streaming decisions, incorporate human-in-the-loop feedback, and align evaluation with financial cost and fairness constraints. Research should prioritize: (1) standardized benchmark protocols (including out-of-time tests), (2) cost-based evaluation that reflects operational losses and investigation capacity, (3) explainable and auditable systems for regulated environments, and (4) privacy-preserving collaboration (e.g., federated learning) to improve generalization without centralizing sensitive data. These directions would strengthen both scientific rigor and practical applicability of ML-based fraud detection.

In terms of funding, the role of government and public institutions is notable. National and international bodies such as the European Commission, Horizon 2020, and the U.S. Army are actively funding ML-based fraud research, acknowledging its relevance for both civilian and defense applications. This aligns with findings from Shou *et al.* (2023) and Sushkov *et al.* (2023), who emphasize fraud detection as a strategic priority for national cybersecurity and economic stability.

In conclusion, the study reveals that machine learning has transformed the landscape of fraud detection by introducing tools that are scalable, adaptive, and increasingly accurate. Nonetheless, key challenges such as model transparency, data imbalance, real-time scalability, and fragmented research still persist. Future work must prioritize explainability, cross-domain generalization, and interdisciplinary collaboration to ensure that fraud detection systems are not only technologically advanced but also ethically and operationally viable. This review contributes to this endeavor by mapping the current terrain, identifying gaps, and laying the groundwork for more unified and impactful research in the future.

Conclusion

In conclusion, this study presents a comprehensive synthesis of 106 Scopus-indexed articles examining the application of machine learning (ML) techniques in detecting fraud. The review identifies a clear and growing interest in this domain, especially since 2020, driven by the increasing complexity of digital financial environments and the limitations of traditional rule-based fraud detection systems. Machine learning offers powerful capabilities for identifying subtle, nonlinear patterns in large datasets through supervised, unsupervised, and hybrid models. Despite the considerable progress made, particularly in areas like deep learning, ensemble modeling, and anomaly detection significant challenges remain, including issues of model explainability, class imbalance, real-time detection, and generalizability across domains. The literature also shows fragmentation in methodology and evaluation metrics, underscoring the need for standardized frameworks and interdisciplinary collaboration. While countries like India, China, and the U.S. lead in contributions, many regions remain underrepresented, highlighting opportunities for more inclusive global cooperation. This study reinforces the need for future research

to prioritize transparency through explainable AI (XAI), develop adaptive real-time detection systems, and ensure model robustness across diverse financial contexts. Overall, this state-of-the-art review not only consolidates fragmented findings but also lays the groundwork for a more unified, ethical, and effective approach to combating fraud using machine learning technologies.

In summary, the main academic value of this SLR is not only in aggregating evidence on ML techniques for fraud detection, but in advancing how the field evaluates and reports evidence. By synthesizing finance- and management-relevant studies from Scopus (2009–2025), this review provides an updated baseline of the literature, introduces an integrative perspective that connects methods, domains, data issues, and evaluation protocols, and highlights why many reported results may not generalize under real operational constraints such as concept drift, investigation capacity, regulatory explainability, and data privacy. These insights support theory development on technology-enabled fraud control and offer methodological guidance for future empirical work to produce results that are more comparable, reproducible, and deployable.

Reference

Aboelfotoh, A., Zamel, A. M., Abu-Musa, A. A., Sabry, S. H., & Moubarak, H. (2025). Examining the ability of big data analytics to investigate financial reporting quality: a comprehensive bibliometric analysis. Journal of Financial Reporting and Accounting, 23(2), 444–471. https://doi.org/10.1108/JFRA-11-2023-0689

Aiemsuwan, P., & Srikamdee, S. (2024). A Novel Hybrid Method for Imbalanced Automobile Insurance Fraud Detection. KST 2024 - 16th International Conference on Knowledge and Smart Technology, 12–17. https://doi.org/10.1109/KST61284.2024.10499643

Alicia, R., Setiawan, T., Breliastiti, R., & Bwarleling, T. H. (2025). ARTIFICIAL INTELLIGENCE (AI): HELPING OR THREATENING AUDITORS?(CASE IN INDONESIA). Jurnal Bina Akuntansi, 12(2), 72-82. https://doi.org/10.52859/jba.v12i2.752

Alsuwailem, A. A. S., Salem, E., & Saudagar, A. K. J. (2023). Performance of Different Machine Learning Algorithms in Detecting Financial Fraud. Computational Economics, 62(4), 1631–1667. https://doi.org/10.1007/s10614-022-10314-x

Appavu, N. (2025). AI and ML Approaches for Credit Card Fraud Detection: A Comparative Study of Logistic Regression and Decision Tree Techniques. 3rd International Conference on Intelligent Data Communication Technologies and Internet of Things, IDCIoT 2025, 2068–2074. https://doi.org/10.1109/IDCIOT64235.2025.10915092

Banerjee, D., & Menon, R. (2019). Complete rare event specification using stochastic treatment: CRESST. In M. A. Wani, T. M. Khoshgoftaar, D. Wang, H. Wang, & N. Seliya (Eds.), Proceedings - 18th IEEE International Conference on Machine Learning and Applications, ICMLA 2019 (pp. 734–739). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICMLA.2019.00131

Bao, Y., Hilary, G., & Ke, B. (2022). Artificial Intelligence and Fraud Detection. In Springer Series in Supply Chain Management (Vol. 11, pp. 223–247). Springer Nature. https://doi.org/10.1007/978-3-030-75729-8_8

Bao, Y., Ke, B., Li, B., Yu, Y. J., & Zhang, J. (2021). A response to "critique of an article on machine learning in the detection of accounting fraud." Econ Journal Watch, 18(1), 71–78. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85104115396&partnerID=40&md5=62b8e82fcaccf16c9adc7bcbe8321d64

Chen, X., & Zhai, C. (2023). Bagging or boosting? Empirical evidence from financial statement fraud detection. Accounting and Finance, 63(5), 5093–5142. https://doi.org/10.1111/acfi.13159

Debener, J., Heinke, V., & Kriebel, J. (2023). Detecting insurance fraud using supervised and unsupervised machine learning. Journal of Risk and Insurance, 90(3), 743–768. https://doi.org/10.1111/jori.12427

Detthamrong, U., Chansanam, W., Boongoen, T., & Iam-On, N. (2024). Enhancing Fraud Detection in Banking using Advanced Machine Learning Techniques. International Journal of Economics and Financial Issues, 14(5), 177–184. https://doi.org/10.32479/ijefi.16613

Dewi, S., & Safitri, A. (2025). Faktor–Faktor Yang Mempengaruhi Penerimaan Opini Audit Going Concern Pada Perusahaan Manufaktur Yang Terdaftar Di Bursa Efek Indonesia. Jurnal Bina Akuntansi, 12(1), 148-157. https://doi.org/10.52859/jba.v12i1.709

Ding, N., Ruan, X., Wang, H., & Liu, Y. (2025). Automobile Insurance Fraud Detection Based on PSO-XGBoost Model and Interpretable Machine Learning Method. Insurance: Mathematics and Economics, 120, 51–60. https://doi.org/10.1016/j.insmatheco.2024.11.006

El Hlouli, F. Z., Riffi, J., Sayyouri, M., Mahraz, M. A., Yahyaouy, A., El Fazazy, K., & Tairi, H. (2023). Detecting Fraudulent Transactions Using Stacked Autoencoder Kernel ELM Optimized by the Dandelion Algorithm. Journal of Theoretical and Applied Electronic Commerce Research, 18(4), 2057–2076. https://doi.org/10.3390/jtaer18040103

Erratum to: Detecting Accounting Fraud in Publicly Traded U.S. Firms Using a Machine Learning Approach (Journal of Accounting Research, (2020), 58, 1, (199-235), 10.1111/1475-679X.12292). (2022). Journal of Accounting Research, 60(4), 1635–1646. https://doi.org/10.1111/1475-679X.12454

Ezeme, O. M., Mahmoud, Q. H., & Azim, A. (2019). A deep learning approach to distributed anomaly detection for edge computing. In M. A. Wani, T. M. Khoshgoftaar, D. Wang, H. Wang, & N. Seliya (Eds.), Proceedings - 18th IEEE International Conference on Machine Learning and Applications, ICMLA 2019 (pp. 992–999). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICMLA.2019.00169

Faatin, F. N., Eltivia, N., & Riwajanti, N. I. (2024). Pengaruh Profitabilitas, Solvabilitas, dan Audit Tenure Terhadap Audit Delay (Studi Pada Sektor Teknologi Di Bursa Efek Indonesia periode 2018-2022). Jurnal Bina Akuntansi, 11(1), 136-153. https://doi.org/10.52859/jba.v11i1.594

Gadde, A., Kishore, G. D. K., Talari, T., Nunna, S. L., Nannapaneni, R. C., & Vamsi, K. M. S. K. (2024). Detecting Deepfake Images: A Deep Learning Approach with Streamlit Integration. Proceedings of 2024 International Conference on Science, Technology, Engineering and Management, ICSTEM 2024. https://doi.org/10.1109/ICSTEM61137.2024.10560646

Galiautdinov, R. (2023). Securing the future of artificial intelligence: A comprehensive overview of ai security measures. In The Use of Artificial Intelligence in Digital Marketing: Competitive Strategies and Tactics (pp. 188–207). IGI Global. https://doi.org/10.4018/978-1-6684-9324-3.ch008

Ghazi, M. R., & Raghava, N. S. (2022). Detecting Ransomware Attacks in Cloud Environment Using Machine Learning-Based Intelligence System in COVID-19 Chaos. 2022 IEEE Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation, IATMSI 2022. https://doi.org/10.1109/IATMSI56455.2022.10119441

Ghosh, S., Bilgaiyan, S., Gourisaria, M. K., & Sharma, A. (2023). Comparative Analysis of Applications of Machine Learning in Credit Card Fraud Detection. 2023 6th International Conference on Information Systems and Computer Networks, ISCON 2023. https://doi.org/10.1109/ISCON57294.2023.10112099

Gupta, S., & Mehta, S. K. (2024). Data Mining-based Financial Statement Fraud Detection: Systematic Literature Review and Meta-analysis to Estimate Data Sample Mapping of Fraudulent Companies Against Non-fraudulent Companies. Global Business Review, 25(5), 1290–1313. https://doi.org/10.1177/0972150920984857

Hamisu, M., & Mansour, A. (2021). Detecting advance fee fraud using NLP bag of word model. Proceedings of the 2020 IEEE 2nd International Conference on Cyberspace, CYBER NIGERIA 2020, 94–97. https://doi.org/10.1109/CYBERNIGERIA51635.2021.9428793

Hernandez Aros, L., Bustamante Molano, L. X., Gutierrez-Portela, F., Moreno Hernandez, J. J., & Rodríguez Barrero, M. S. (2024). Financial fraud detection through the application of machine learning techniques: a literature review. Humanities and Social Sciences Communications, 11(1). https://doi.org/10.1057/s41599-024-03606-0

Hoseini, C., Badar, M. A., Shahhosseini, A. M., & Kluse, C. J. (2021). A review of machine learning methods applicable to quality issues. Proceedings of the International Conference on Industrial Engineering and Operations Management, 1225–1240. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85114228484&partnerID=40&md5=ea7cbac3b0d53d8a9215bcb629a68690

Hudnurkar, M., Singh, K., Ambekar, S., Sahu, G., & Yecho, H. (2024). Legalities in Metaverse - Ethereum Fraud Detection. Proceedings of 9th International Conference on Science, Technology, Engineering and Mathematics: The Role of Emerging Technologies in Digital Transformation, ICONSTEM 2024. https://doi.org/10.1109/ICONSTEM60960.2024.10568862

Ibrahim, R., & Badr, I. (2025). Investigating the Role of AI Techniques in CCFD: A Quantitative Study in the Accounting and Finance Sector. In From Digital Disruption to Dominance: Leveraging FinTech Applications for Sustainable Growth (pp. 133–162). Emerald Group Publishing Ltd. https://doi.org/10.1108/978-1-83549-608-420251006

Jaidhan, B. J., Divya Madhuri, B., Pushpa, K., Lakshmi Devi, B. V. S., & Shanmuk Srinivas, A. (2019). Application of big data analytics and pattern recognition aggregated with random forest for detecting fraudulent credit card transactions (CCFD-BPRRF). International Journal of Recent Technology and Engineering, 7(6), 1082–1087. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85064938994&partnerID=40&md5=e3468c8f3c15723cc107e0f77f9c1915

Kini, A., Chelluru, R., Naik, K., Naik, D., Aswale, S., & Shetgaonkar, P. (2022). Automobile Insurance Fraud Detection: An Overview. Proceedings of 3rd International Conference on Intelligent Engineering and Management, ICIEM 2022, 7–12. https://doi.org/10.1109/ICIEM54221.2022.9853043

Knuth, T., & Ahrholdt, D. C. (2022). Consumer Fraud in Online Shopping: Detecting Risk Indicators through Data Mining. International Journal of Electronic Commerce, 26(3), 388–411. https://doi.org/10.1080/10864415.2022.2076199

Kolodiziev, O., Mints, A., Sidelov, P., Pleskun, I., & Lozynska, O. (2020). AUTOMATIC MACHINE LEARNING ALGORITHMS FOR FRAUD DETECTION IN DIGITAL PAYMENT SYSTEMS. Eastern-European Journal of Enterprise Technologies, 5(107), 14–26. https://doi.org/10.15587/1729-4061.2020.212830

Lata Jeyaraj, S. A., Revathy, S., Jayabalan, K., Sandeep, K. M., Yenigalla, G., & Krishna, K. B. (2024). Machine Learning Algorithms for ECommerce Security: A Practical Approach. In Strategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning (pp. 361–385). IGI Global. https://doi.org/10.4018/979-8-3693-6557-1.ch015

Li, W., Chen, H., & Nunamaker, J. F. (2016). Identifying and Profiling Key Sellers in Cyber Carding Community: AZSecure Text Mining System. Journal of Management Information Systems, 33(4), 1059–1086. https://doi.org/10.1080/07421222.2016.1267528

Li, W., Liu, X., Su, J., & Cui, T. (2025). Advancing financial risk management: A transparent framework for effective fraud detection. Finance Research Letters, 75. https://doi.org/10.1016/j.frl.2025.106865

Lin, J., Guo, X., Zhu, Y., Mitchell, S., Altman, E., & Shun, J. (2024). FraudGT: A Simple, Effective, and Efficient Graph Transformer for Financial Fraud Detection. ICAIF 2024 - 5th ACM International Conference on AI in Finance, 292–300. https://doi.org/10.1145/3677052.3698648

Lin, W.-H., Wang, P., & Tsai, C.-F. (2016). Face recognition using a support vector model classifier for user authentication. Electronic Commerce Research and Applications, 18, 71–82. https://doi.org/10.1016/j.elerap.2016.01.005

Lokanan, M., Tran, V., & Vuong, N. H. (2019). Detecting anomalies in financial statements using machine learning algorithm: The case of Vietnamese listed firms. Asian Journal of Accounting Research, 4(2), 181–201. https://doi.org/10.1108/AJAR-09-2018-0032

Loughran, T., & McDonald, B. (2020). Textual Analysis in Finance. Annual Review of Financial Economics, 12, 357–375. https://doi.org/10.1146/annurev-financial-012820-032249

Loukili, M., Messaoudi, F., & Azirar, H. (2024). E-Payment Fraud Detection in E-Commerce using Supervised Learning Algorithms. In Advances in Emerging Financial Technology and Digital Money (pp. 27–35). CRC Press. https://doi.org/10.1201/9781032667478-3

Loukili, M., Messaoudi, F., & El Ghazi, M. (2024). Defending against digital thievery: a machine learning approach to predict e-payment fraud. International Journal of Management Practice, 17(5), 522–538. https://doi.org/10.1504/IJMP.2024.140861

Lu, M., Han, Z., Rao, S. X., Zhang, Z., Zhao, Y., Shan, Y., Raghunathan, R., Zhang, C., & Jiang, J. (2022). BRIGHT - Graph Neural Networks in Real-time Fraud Detection. International Conference on Information and Knowledge Management, Proceedings, 3342–3351. https://doi.org/10.1145/3511808.3557136

Mansour, N., & M, B. V. L. (Eds.). (2024). 3rd Finance, Accounting, and Law in the Digital Age Conference, 2024. In Springer Proceedings in Business and Economics. Springer Nature. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85208246345&partnerID=40&md5=1f3e370b37abf867e36d240a3f68c9d5

Medarhri, I., Hosni, M., Ettalhaoui, M., Belhaj, Z., & Zine, R. (2024). Reviewing Machine Learning Techniques in Credit Card Fraud Detection. In F. Coenen, A. Fred, & J. Bernardino (Eds.), International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management, IC3K - Proceedings (Vol. 1, pp. 179–187). Science and Technology Publications, Lda. https://doi.org/10.5220/0013072500003838

Mirhashemi, Q. S., Nasiri, N., & Keyvanpour, M. R. (2023). Evaluation of Supervised Machine Learning Algorithms for Credit Card Fraud Detection: A Comparison. 2023 9th International Conference on Web Research, ICWR 2023, 247–252. https://doi.org/10.1109/ICWR57742.2023.10139098

Mishra, K. N., Mishra, V. P., Saket, S., & Mishra, S. P. (2022). Hybrid approach for deception tracing in smart cities using LR and n-fold intelligent machine learning techniques. International Journal of Management Practice, 15(4), 460–487. https://doi.org/10.1504/IJMP.2022.10048751

Pandey, A. (2024). Retrieval Augmented Fraud Detection. ICAIF 2024 - 5th ACM International Conference on AI in Finance, 328–335. https://doi.org/10.1145/3677052.3698692

Papík, M., & Papíková, L. (2022). Detecting accounting fraud in companies reporting under US GAAP through data mining. International Journal of Accounting Information Systems, 45. https://doi.org/10.1016/j.accinf.2022.100559

Patel, S., Pandey, M., & Rajeswari, D. (2024). Fraud Detection in Financial Transactions: A Machine Learning Approach. Proceedings of 9th International Conference on Science, Technology, Engineering and Mathematics: The Role of Emerging Technologies in Digital Transformation, ICONSTEM 2024. https://doi.org/10.1109/ICONSTEM60960.2024.10568903

Poursafaei, F., Hamad, G. B., & Zilic, Z. (2020). Detecting Malicious Ethereum Entities via Application of Machine Learning Classification. 2020 2nd Conference on Blockchain Research and Applications for Innovative Networks and Services, BRAINS 2020, 120–127. https://doi.org/10.1109/BRAINS49436.2020.9223304

Qiu, S., & Luo, Y. (2024). How to detect and forecast corporate fraud by media reports? An approach using machine learning and qualitative comparative analysis. Journal of Forecasting, 43(1), 58–80. https://doi.org/10.1002/for.3022

Ramadhana, R. N., Sari, K. R., & Wahyudi, R. (2024). Pengaruh Penerapan Pengendalian Internal, Audit Investigasi Dan Akuntansi Forensik Terhadap Pengungkapan Kecurangan Pada Pemerintah Kabupaten Bali. Jurnal Bina Akuntansi, 11(1), 18-32. https://doi.org/10.52859/jba.v11i1.587

Riskiyadi, M. (2024). Detecting future financial statement fraud using a machine learning model in Indonesia: a comparative study. Asian Review of Accounting, 32(3), 394–422. https://doi.org/10.1108/ARA-02-2023-0062

Saheed, Y. K., Baba, U. A., & Raji, M. A. (2022). Big Data Analytics for Credit Card Fraud Detection Using Supervised Machine Learning Models. In Big Data Analytics in the Insurance Market (pp. 31–56). Emerald Group Publishing Ltd. https://doi.org/10.1108/978-1-80262-637-720221003

Sankar, S., Subash, V., Princy, P., Vishalkumar, G., Booma, S., & Solayappan, A. (2024). A Novel Method for Detecting Financial Fraud Using Deep Learning in Online Retail. Proceedings of 9th International Conference on Science, Technology, Engineering and Mathematics: The Role of Emerging

Technologies in Digital Transformation, ICONSTEM 2024. https://doi.org/10.1109/ICONSTEM60960.2024.10568906

Sari, F. M., Elshifa, A., & Mulyapradana, A. (2025). Analisis Determinan Fraud Dalam Distribusi Bantuan Sosial: Perspektif Fraud Triangle. Jurnal Bina Akuntansi, 12(1), 33-47. https://doi.org/10.52859/jba.v12i1.702

Sharma, O., & Pandey, N. (2023). Machine Learning and Blockchain for Security Management in Banking System. In Computational Intelligence for Cybersecurity Management and Applications (pp. 65–81). CRC Press. https://doi.org/10.1201/9781003319917-6

Shi, F., & Zhao, C. (2023). Enhancing financial fraud detection with hierarchical graph attention networks: A study on integrating local and extensive structural information. Finance Research Letters, 58. https://doi.org/10.1016/j.frl.2023.104458

Shirgave, S. K., Awati, C. J., More, R., & Patil, S. S. (2019). A review on credit card fraud detection using machine learning. International Journal of Scientific and Technology Research, 8(10), 1217–1220. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85074036448&partnerID=40&md5=19adddfc934ed8a51ecf6a658e05f62c

Shou, M., Bao, X., & Yu, J. (2023). An optimal weighted machine learning model for detecting financial fraud. Applied Economics Letters, 30(4), 410–415. https://doi.org/10.1080/13504851.2021.1989367

Subramaniam, G. A. L., Mahmoud, M. A., Abdulwahid, S. N., & Gunasekaran, S. S. (2024). A Location-Based Fraud Detection in Shipping Industry Using Machine Learning Comparison Techniques. In Studies in Systems, Decision and Control (Vol. 553, pp. 15–26). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-031-67317-7_2

Sushkov, V. M., Leonov, P. Y., Nadezhina, O. S., & Blagova, I. Y. (2023). Integrating Data Mining Techniques for Fraud Detection in Financial Control Processes. International Journal of Technology, 14(8), 1675–1684. https://doi.org/10.14716/ijtech.v14i8.6830

Tayebi, M., & El Kafhali, S. (2025). Combining Autoencoders and Deep Learning for Effective Fraud Detection in Credit Card Transactions. Operations Research Forum, 6(1). https://doi.org/10.1007/s43069-024-00409-6

Trozze, A., Kleinberg, B., & Davies, T. (2024). Detecting DeFi securities violations from token smart contract code. Financial Innovation, 10(1). https://doi.org/10.1186/s40854-023-00572-5

Vandervorst, F., Verbeke, W., & Verdonck, T. (2022). Data misrepresentation detection for insurance underwriting fraud prevention. Decision Support Systems, 159. https://doi.org/10.1016/j.dss.2022.113798

Vičič, J., & Tošić, A. (2022). Application of Benford's Law on Cryptocurrencies. Journal of Theoretical and Applied Electronic Commerce Research, 17(1), 313–326. https://doi.org/10.3390/jtaer17010016

Walker, S. (2021). Critique of an article on machine learning in the detection of accounting fraud. Econ Journal Watch, 18(1), 61–70. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85104149275&partnerID=40&md5=421a8116d804d91ffd44258143bf6b08

Wang, Y., & Xu, W. (2018). Leveraging deep learning with LDA-based text analytics to detect automobile insurance fraud. Decision Support Systems, 105, 87–95. https://doi.org/10.1016/j.dss.2017.11.001

Wijaya, J. R. T., & Herwiyanti, E. (2023). A study of information asymmetry in financial research. The Indonesian Accounting Review, 13(1), 79-89.

Wijaya, J. R. T., & Manurung, M. R. A. (2025). The Impact of Digitalization on Financial Accounting Practices: A Literature Review in the Scopus Database. Review of Applied Accounting Research (RAAR), 5(1), 53-70.

Wijaya, J. R. T., Prasetyo, I., Rahmatika, D. N., & Indriasih, D. (2025). ARTIFICIAL INTELLIGENCE AND AUDIT QUALITY: AN EMPIRICAL LITERATURE REVIEW FROM SCOPUS DATABASE. Fokus Ekonomi: Jurnal Ilmiah Ekonomi, 20(1), 61-76.

Wiryadinata, D., & Sugiharto, A. (2023). The Use of Machine Learning to Detect Financial Transaction Fraud: Multiple Benford Law Model for Auditors. Journal of Information Systems Engineering and Business Intelligence, 9(2), 239–252. https://doi.org/10.20473/jisebi.9.2.239-252

Zhai, J., Cao, Y., Yao, Y., Ding, X., & Li, Y. (2017). Computational intelligent hybrid model for detecting disruptive trading activity. Decision Support Systems, 93, 26–41. https://doi.org/10.1016/j.dss.2016.09.003

Zhao, D., Wang, Z., Schweizer-Gamborino, F., & Sornette, D. (2025). Polytope Fraud Theory. International Review of Financial Analysis, 97. https://doi.org/10.1016/j.irfa.2024.103734

Zhu, S., Ma, T., Wu, H., Ren, J., He, D., Li, Y., & Ge, R. (2025). Expanding and Interpreting Financial Statement Fraud Detection Using Supply Chain Knowledge Graphs. Journal of Theoretical and Applied Electronic Commerce Research, 20(1). https://doi.org/10.3390/jtaer20010026

Zkik, K., Sebbar, A., Fadi, O., Kamble, S., & Belhadi, A. (2024). Securing blockchain-based crowdfunding platforms: an integrated graph neural networks and machine learning approach. Electronic Commerce Research, 24(1), 497–533. https://doi.org/10.1007/s10660-023-09702-8