Intelligent Systems, Machine Learning, and Deep Learning Algorithms for Detecting Banking Fraud: A Review

Jessica Vazallo-Bautista, Allison Villalobos-Peña, Juan Soria-Quijaite
Escuela de Ingeniería de Sistemas, Universidad Tecnológica del Perú, Lima, Perú

***Abstract*—The increase in unauthorized remote banking fraud has intensified with the expansion of digital channels, creating new risks and highlighting the inadequacy of traditional methods based on fixed rules and manual audits. This review aims to synthesize recent scientific evidence on the use of machine learning and deep learning techniques for the early detection of fraudulent banking transactions, considering supervised and unsupervised models and deep architectures that allow the analysis of complex patterns present in financial transactions. A total of 357 original articles were identified in the Scopus and Web of Science databases, in addition to manual research, published up to 2025. Of these, 35 studies met the inclusion criteria established using the PICOT approach and the PRISMA protocol. The most widely implemented models in the selected studies were Random Forest, XGBoost, SVM, LSTM networks, and graph-based approaches. The combination of different algorithms improves fraud detection by integrating temporal, relational, and behavioral patterns. Advanced models show better metrics in accuracy, recall, and F1-score compared to traditional methods, expanding the possibilities for continuous monitoring and reducing false positives. There are consistent associations between the application of advanced models, the availability of quality data, and the ability to adapt to different transactional scenarios, which favor timely fraud detection if challenges such as class imbalance, the need for real-time decisions, and the heterogeneity of financial contexts are addressed. The integration of multiple approaches and the optimization of preprocessing and evaluation processes allow us to move toward more robust, scalable anti-fraud systems that are better suited to the current demands of the digital environment.**

***Keywords*—Deep learning; algorithms; machine learning; fraud detection; real-time methods**

I. Introduction

Today, unauthorized remote banking fraud is one of the main threats to the stability of the financial system, as fraudsters use digital channels such as online banking, mobile banking, and telephone banking to illegally access customer accounts and make unauthorized transfers. This situation is exacerbated by the increasing digitization of financial services and the rise in the volume of online transactions, which exposes banking institutions to increasingly complex vulnerabilities [1].

Faced with this problem, IT security in the banking sector has become extremely important. The use of machine learning (ML) and deep learning (DL) techniques has made it possible to overcome many of the limitations of traditional rule-based systems, which tend to be rigid and ineffective against rapidly evolving attacks [2]. Furthermore, these methodologies have been shown to be useful not only in the financial sector, but also in other areas where they have been successfully applied in systematic reviews to solve large-scale problems [3]. Several recent studies have analyzed advances in the use of ML and DL applied to financial fraud. Husnaningtyas and Dewayanto [4] , evaluated the performance of unsupervised learning algorithms in detecting fraud within financial transactions, highlighting their effectiveness in identifying hidden patterns and irregular behavior in large volumes of data. Similarly, Yanto, Lisah, and Tandra [5], examined different supervised learning models, concluding that approaches such as Random Forest, XGBoost, and short-term and long-term memory (LSTM) are the most accurate and widely used in fraud detection, although with a limitation in terms of their real-time response capacity. Despite their advances, these methods still face obstacles in practice. Although they have been proven to process large volumes of data and uncover hidden patterns, many models cannot detect operations in real time and have difficulty adapting to class imbalance. This highlights the need to create anti-fraud models that are adaptive, scalable, and capable of working online efficiently [6]. Traditional solutions, such as static rules or manual audits, have proven to be completely inadequate. Not only do they generate a large number of false positives, but they also lack flexibility and fail to adapt quickly to changes in fraudsters' tactics [7].

In contrast, ML and DL algorithms have transformed the way banking fraud is addressed. Supervised models can differentiate between legitimate and fraudulent transactions, while unsupervised models identify anomalies that had not been previously classified [8].

Deep architectures, such as recurrent neural networks (RNN), LSTM, and convolutional neural networks (CNN), have also made a difference. These networks capture temporal and multivariate patterns, improving the accuracy and scalability of systems. In addition, they enable the development of hybrid models capable of processing transactions more quickly and in real time [9]. Empirical results reinforce these contributions. Semi-supervised graph models have been applied to detect suspicious connections with incomplete data [10]. Furthermore, comparisons between classical algorithms and deep models have shown that the latter are better at capturing the temporal dynamics of fraud [11].

Likewise, it has been proven that classifier assembly techniques help improve robustness in contexts with highly unbalanced data [12]. In addition, graph-based models with

attention networks have made it possible to uncover hidden relationships between customers, businesses, and organized fraud [13]. Working with real data has also been key. Zioviris, Kolomvatsos, and Stamoulis [14] , at a Moroccan bank showed that applying oversampling to unbalanced data and combining it with supervised classifiers achieved more effective results in fraud detection. However, there are still gaps. Many studies focus on specific techniques or datasets, which limits their applicability. In addition, there is often little attention paid to metrics that are more useful in practice, such as recall, F1-score, AUC, and latency, which are crucial for measuring effectiveness in real time.

For these reasons, the objective of this systematic review is to identify, analyze, and classify intelligent systems and machine learning and deep learning algorithms applied to the early detection of banking fraud in real time. It also seeks to synthesize performance metrics, trends, and challenges in order to provide a frame of reference to guide both future research and practical implementation in the financial industry.

II. Methodology

In the systematic review, the PICOT method was used to search for scientific articles, as it allows questions to be formulated based on the problem addressed through its components: Problem (P), Intervention (I), Comparison (C), Outcomes (O), and Time (T). Its application allows for the clear establishment of inclusion and exclusion criteria, ensuring relevance and rigor in the selection of the articles analyzed.

A. PICOT Formulation

During the first phase of the methodological process, the PICOT components were identified, as summarized in Table I, and a complementary Context variable was also incorporated for a more precise search.

TABLE I. Identification of Picot Components

P	Financial transactions susceptible to bank fraud.
I	Application of intelligent systems and Machine Learning and Deep Learning algorithms.
C	Conventional methods of fraud detection.
O	Performance and efficiency in detecting bank fraud using algorithms.
T	Speed and timeliness of detection.

B. Question Formulation

Once the PICOT components had been identified, the general research question (RQ) for this systematic review was formulated:

"What Machine Learning (ML) and Deep Learning (DL) models have been developed for the early detection of banking fraud in real-time, and how have they performed in terms of accuracy, efficiency, and resource optimization compared to traditional methods?"

Subsequently, specific questions linked to each PICOT component were designed to guide the literature search and ensure the relevance of the selected studies. These questions are summarized in Table II.

TABLE II. Questions Linked to PICOT Components

RQ1	What are the main types of bank fraud (suspicious transactions, digital payments, card fraud) addressed in recent studies?
RQ2	What machine learning and deep learning models have been developed for the early detection of banking fraud in real time?
RQ3	What are the differences in performance between intelligent ML/DL models and traditional methods (static rules, manual monitoring, conventional audits)?
RQ4	What metrics of precision, accuracy, efficiency, early detection, and reliability have been reported by the applied models?
RQ5	Which models enable immediate fraud detection, either online or through continuous real-time monitoring?

C. Identification of Keywords

The keywords for each PICOT component were identified and are presented in Table III. Thesauri were used for this purpose, along with the Boolean operators "OR" and double quotation marks ("") to facilitate the search for exact terms in the Scopus and WOS databases.

TABLE III. Keywords

P	"Banking transactions" OR "Bank fraud" OR "Digital payment fraud" OR "Credit card fraud"
I	"Machine learning" OR "Deep learning" OR "Artificial intelligence" OR "Supervised learning" OR "Support vector machine (SVM)"
C	"Traditional methods" OR "Manual monitoring" OR "Classic statistical methods" OR "Conventional auditing"
O	"Precision" OR "Accuracy" OR "Efficiency" OR "Early detection" OR "Reliability" OR "Resource optimization"
T	"Real time" OR "Immediate" OR "Online detection" OR "Continuous monitoring" OR "Instant evaluation"

D. Syntax of the PICOT Formula

The PICOT method was completed by combining all the previously identified keywords using the Boolean operator "AND" to perform the correct search in the Scopus and Web of Science databases, finding the search equations shown in Table IV.

TABLE IV. Search Equation

	Scopus	Web of Science
Busqueda equidad	TITLE-ABS-KEY("Transacciones bancarias" O "Fraude bancario" O "Fraude en pagos digitales" O "Fraude con tarjetas de crédito") AND TITLE-ABS-KEY("Machine learning" OR "Deep learning" OR "Artificial intelligence" OR "Supervised learning" OR "Support vector machine (SVM)") AND TÍTULO-ABS-CLAVE("Métodos tradicionales" O "Monitoreo manual" O "Métodos estadísticos clásicos" O "Auditoría convencional") AND TÍTULO-ABS-CLAVE("Precisión" O "Exactitud" O "Eficiencia" O "Detección temprana" O "Fiabilidad" O "Optimización de recursos") AND TÍTULO-ABS-CLAVE("Tiempo real" O "Inmediato" O "Detección en línea" O "Monitoreo continuo" O	(((((((TS = banking transactions) OR (TS = bank fraud)) OR (TS = digital payment fraud)) OR (TS = credit card fraud)) AND (((((TS = machine learning) OR (TS = deep learning)) OR (TS = artificial intelligence)) OR (TS = supervised learning)) OR ((TS = support vector machine) AND (TS = svm)))) AND ((((TS = traditional methods) OR (TS = manual monitoring)) OR (TS = classic statistical methods)) OR (TS = conventional auditing))) AND ((((((TS = precision) OR (TS = accuracy)) OR (TS = efficiency)) OR (TS = early detection)) OR (TS = reliability)) OR ((SO_SMART = optimization) AND (TS = resource)))) AND (((((TS = real

	"Evaluación instantánea") Y (LÍMITE A (SUBJAREA,"COMP")) Y (LÍMITE A (DOCTYPE,"ar")) Y (LÍMITE A (OA,"all")) Y (LÍMITE A (IDIOMA,"Español")) Y AÑO PUBLICITARIO > 2020 Y AÑO PUBLICITARIO < 2025	time) OR (TS = immediate)) OR (TS = online detection)) OR (TS = continuous monitoring)) OR (TS = instant evaluation)))

Once the PICOT method was completed and the search strategies were executed in the database, a total of 357 articles were obtained: 290 from Scopus and 67 from the Web of Science (WOS) database.

E. Specifications of Inclusion and Exclusion Criteria

In order to ensure the validity, relevance, and quality of the selected studies, inclusion and exclusion criteria were defined. These criteria allowed the review to focus on research directly related to the application of Machine Learning (ML) and Deep Learning (DL) models in the detection of bank fraud, thus ensuring consistency in the results. In terms of inclusion criteria, studies published between 2021 and 2025 in indexed scientific journals and specialized conference proceedings were selected, whose subject matter was related to the use of Machine Learning (ML) and Deep Learning (DL) techniques applied to bank fraud, including both financial transactions and fraud associated with digital payments and credit card use. It was also considered essential that the research presented performance evaluation metrics, such as precision, accuracy, sensitivity, specificity, recall, F1-score, or area under the curve (AUC), and that it incorporated approaches aimed at real-time detection, either online or through continuous monitoring schemes. Finally, only articles published in English or Spanish that offered full access to the text were included. With regard to exclusion criteria, duplicate studies or those corresponding to preliminary versions already published in other sources were discarded, as were studies published prior to 2021. Research that did not directly address the issue of bank fraud, studies that lacked quantitative performance metrics, and documents that were not fully accessible were also excluded. The application of these parameters ensured the methodological consistency of the review, refined the database of articles collected, and ensured the quality and relevance of the evidence analyzed.

F. PRISMA Statement

The PRISMA statement enabled the selection and analysis of articles, as well as the establishment of a process for extracting the articles to be examined in the literature review, ensuring consistency between the objectives and the criteria established. This approach guarantees transparency and comprehensiveness in the identification, selection, and synthesis of the included studies, which strengthens the validity of the methodology [15].

Likewise, Moher et al. [16] emphasizes that the correct application of the 27 items in the PRISMA statement allows for the standardization of the processes of searching, analyzing, and evaluating articles, promoting comparability between studies. This standardization is essential to ensure the consistency and quality of systematic reviews, as it promotes transparency in the presentation of results.

G. PRISMA Processes

The development was carried out in five stages. First, 357 articles were identified (290 from Scopus and 67 from WOS) and 40 duplicates were removed using Mendeley. Subsequently, 272 studies were excluded after analyzing unrelated titles and abstracts. Ten additional records were discarded because they did not meet the PICOT criteria. Finally, 35 articles relevant to the review were selected. Fig. 1 shows the comprehensive article selection process, using the PRISMA diagram, where 35 articles were selected.

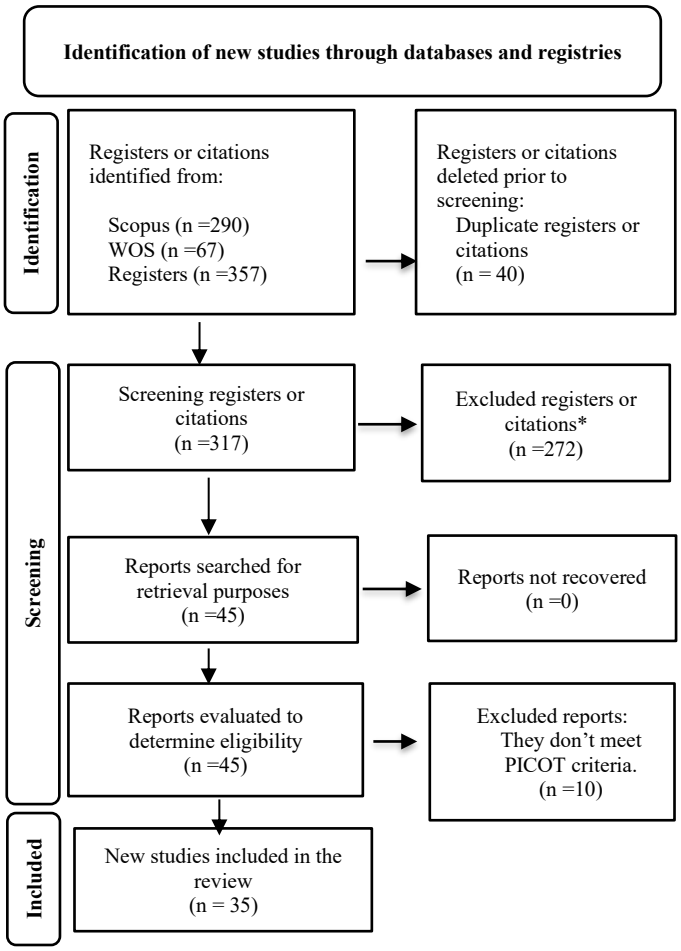

Fig. 1. Diagram of the PRISMA process.

H. Bibliometrix by R Studio

Bibliometric analysis has established itself as an essential tool for studying the evolution of knowledge about bank fraud. Using Bibliometrix in R, databases such as Scopus can be analyzed to identify trends, authors, and emerging topics in financial fraud detection. Shukla and Kashni demonstrated that scientific output on bank fraud has grown over the last decade, highlighting the use of machine learning models [17]. Recent studies show an increase in the use of artificial intelligence and machine learning to detect financial anomalies. Bibliometrix allows these advances to be visualized through co-occurrence and collaboration maps, showing an annual growth of 13.34% in research on AI applied to finance and highlighting gaps in transparency, ethics, and algorithmic biases in automated systems [18], [19].

According to Gangwar, the study of financial crimes, such as money laundering, has grown significantly over the last decade, driven by digitization and the increase in illicit flows. This approach provides an understanding of how technological tools, including artificial intelligence and predictive detection models, are integrated into fraud prevention processes [20].

III. RESULTS

In the results section, tables and graphs were created to visually represent the different categories of characteristics of the elements analyzed. Excel spreadsheets were used for the graphs. In addition, the results address the PICOT questions formulated during the writing of the research.

A. Developed Models

The results of the reviewed articles are shown in Table V, which indicates the reference, types of fraud, and Machine Learning (ML) and Deep Learning (DL) models applied.

B. Real-Time Detection Metrics and Techniques

The results of the reviewed articles are shown in Table VI, which indicates the reference, the metrics for each study result, and the models used for real-time detection.

TABLE V. RESULTS OF THE REVIEWED ARTICLES

Reference	Types of Fraud	ML and DL models
Adejoh, J. et al. (2024)[21]	CNP, skimming, unauthorized digital payments, account takeover, fake accounts, and money laundering using mule accounts.	Random Forest, XGBoost, Isolation Forest, Autoencoders, LSTM/GRU, CNN y Graph Neural Networks (GNN).
Ibrahim, Y. et al. (2025)[22]	Suspicious transactions, card fraud, and anomalous digital payments.	LSTM, CNN, AE, and hybrid ML/DL models enable online detection.
Hargreaves, C. A. (2025)[23]	Card, digital payments, account takeover/money laundering	ML: Logistic, RF, XGBoost/LightGBM/CatBoost. DL: LSTM/GRU, AE, 1D-CNN, GNN; hybrids: rules+ML.
Demirhan, H. (2024)[24]	Credit card fraud: fraudulent or legitimate transactions.	RF, XGBoost, SVM, DNN, LSTM, GNN, and fuzzy logistic regression.
Abd-Ellatif, L. et al. (2025)[25]	Suspicious transactions, digital payments, cards, and financial anomalies.	ML: RF, XGBoost, CatBoost; DL: CNN, RNN, LSTM, GNN
Theodorakopoulos, L. et al. (2025)[26]	credit cards, online payments, and suspicious transactions.	LR, DT, RF, XGBoost, CatBoost; PySpark for scalability and adaptive learning
El-Kenawy, E.-S. M. et al. (2024)[27]	Credit card fraud in electronic transactions.	DL: RNN, LSTM, and GRU applied to balanced Kaggle datasets
Rawashdeh, E. (2024)[28]	Card fraud: duplicates, unauthorized use, and anomalous online purchases.	HybridIG-CSO hybrid model with evolutionary selection and RWN.
Alarfaj, F. K. & Shahzadi, S. (2025)[29]	Fraud: credit cards, digital payments, and suspicious transactions.	Models: LSTM, CNN, AE, XGBoost, CatBoost, and ensembles.
Wang, H. (2024)[30]	Fraud: cards, digital payments, transfers, phishing, and identity theft.	ML: XGBoost, RF, LightGBM; DL: RNN/LSTM/GRU, CNN, AE, Transformers; Hybrids: GNN, CNN-LSTM, ensembles.
Saha, S. C. (2024)[31]	Fraud: cards, unusual transactions, digital payments, and account theft.	Online/lightweight models: Hoeffding Tree, Online RF, IF, incremental OCSVM, compact AEs, LSTM in short windows.
Baisholan, N. et al. (2025)[32]	Fraud: suspicious transactions, digital payments, and cards.	Models: RF, XGBoost, LSTM, CNN, AE, and ML+DL hybrids for real-time early detection.
Brown, J. (2022)[33]	Card fraud, digital payments, and identity theft.	ML/DL: RF, XGBoost, AE, LSTM, CNN, GNN, and streaming models (ARF, Hoeffding Tree).
Al-Maari, A. A. et al. (2025)[34]	Fraud: cards, digital payments, suspicious transactions, and account theft.	Hoeffding Tree, Isolation Forest, real-time LSTM.
Kcennedy, R. K. L. et al. (2024)[35]	Cloning and CNP fraud, transactions in apps/digital wallets, account hijacking, and money laundering.	ML: Logistic, RF, XGBoost/LightGBM/CatBoost; DL: RNN/LSTM/GRU, AE, 1D-CNN; Relational: GNN; Hybrids: rules + ML/DL.
Ibomoiye, D. M., et al. (2024)[36]	Credit card fraud (cloning, unauthorized transactions)	GAN + RNN/LSTM/GRU: GAN creates synthetic fraud, RNN/LSTM/GRU classifies.
Tayebi, M. et al. (2025)[37]	Fraud: cards, digital payments, and account takeover.	ML: Logistic, DT, RF, XGBoost/LightGBM/CatBoost; DL: RNN/LSTM/GRU, AE, 1D-CNN; Relational: GNN; Hybrids: rules + ML/DL.
Cascavilla, G. (2025)[38]	Suspicious transactions (payments, chargebacks, CNP) and atypical behavior, including anomalous digital payments.	Autoencoders, Isolation Forest, One-Class SVM
AbouGrad, H. (2025)[39]	Digital payment fraud and suspicious online banking transactions, with a focus on distributed data.	Decentralized Deep AutoEncoder
Liu, J. (2025)[40]	Main type: card fraud	DNN, CNN, RNN, GRU, LSTM, CCNN.
Ullah, H. (2022)[41]	Credit card fraud, including physical unauthorized use and online transactions (CNP).	Random Forest (RF), XGBoost Classifier, Convolutional Neural Network
Yu, J. (2024)[42]	Card fraud (CNP and unauthorized), suspicious transactions, and digital payments; focused on detecting anomalies in payment flows.	AutoEncoder, LightGBM, SMOTE
Sun, Y. (2023)[43]	It focuses on card fraud (CNP and unauthorized), suspicious transactions, and fraudulent digital payments.	Modelos ML: Random Forest, AdaBoost, XGBoost, LightGBM, CatBoost; DL: MLP, LSTM, GRU.
Al Balawi, S. (2023)[44]	It focuses on card fraud (in-person and CNP) and suspicious transactions.	ANN and CNN, with and without pooling layer.

Alsagri, H. S. (2025)[45]	It focuses on card fraud and fraudulent electronic transactions, concentrating on detecting anomalies in the CCF dataset.	ML: LR, SVM, RF, XGBoost, KNN; DL: DNN.
Akour, I. (2025)[46]	The main focus was on card fraud, especially unauthorized online transactions; the model analyzes sequences to distinguish normal behavior from anomalous patterns.	ML: LR, SVM, RF, ANN; DL: CNN, LSTM, CNN–LSTM, CNN–LSTM with Attention.
Benchaji, I. (2021)[47]	Card fraud, especially in digital transactions, was the most studied; the model identifies anomalies in sequential customer patterns.	The LSTM model outperforms other ML models by capturing temporal dependencies, improving early detection of irregular operations.
Owoh, N. (2024)[48]	Card fraud, especially in digital purchases, with anomalous patterns best detected by intelligent models.	RF, SVM, KNN, Bagging, Boosting, and an Ensemble model were applied.
Strelcenia, E. (2023)[49]	The main type of fraud analyzed is unauthorized use of credit cards in electronic transactions.	XGBoost, RF, KNN, MLP, and Logistic Regression were applied to balanced datasets using SMOTE, ADASYN, and GAN variants (CGAN, WSGAN, NSGAN, LSGAN, SDG-GAN, K-CGAN).
Ren, J. (2024)[50]	Types of fraud: credit/debit cards, digital payments and online banking, suspicious transactions, internal fraud.	DT, RF, GBDT, XGBoost, LightGBM, Stacking Ensemble.
Fedushko, S. (2023)[51]	It focuses on credit card fraud in online transactions.	ML models were developed and compared: LR, RF, DT, SVM, Naïve Bayes, KNN, and SGD Classifier.
Plakandaras, V. (2022)[52]	Primary fraud: credit card transactions in online environments.	Ridge LR (best performance), SVM, RF, DT
Alatawi, M. N. (2025)[53]	Credit card fraud, in person and online, detecting anomalous patterns using IoT features.	Random Forest and Gradient Boosting Machine
Muduli, D. (2025)[54]	Focuses on card fraud and suspicious transactions in Credit-Card and PaySim datasets.	SVM, KNN, ELM, PSO-ELM, and Stacking Ensemble (SVM + KNN + PSO-ELM with Gradient Boosting).
Feng X et al (2024)[55]	Focus: Card fraud and suspicious transactions in transactional datasets (European cardholders).	RF+AB, GBDT, SVM, KNN, CNN; CDL is proposed to reduce features and train traditional/ensemble models, optimizing accuracy and time.

TABLE VI. RESULTS OF REAL-TIME DETECTION METRICS AND TECHNIQUES

Reference	Metrics	Real-time models
Adejoh, J. et al. (2024)[21]	Accuracy (94–99%), Recall, Precision, F1-score, and AUC-ROC are the most commonly used metrics for validating performance.	Models such as Hoeffding Tree, Adaptive Random Forest, and Autoencoders enable real-time detection and monitoring.
Ibrahim, Y. et al. (2025)[22]	Accuracy (94–99%), Recall, Precision, F1-score, and AUC-ROC are the most commonly used metrics for validating performance.	LSTM, CNN, and Autoencoders enable real-time detection and monitoring.
Hargreaves, C. A. (2025)[23]	Accuracy, Precision, Recall, F1, ROC-AUC, AUPRC, MCC, FP rate, inference time (ms), throughput (tx/s).	XGBoost, LightGBM, Logistic, Random Forest, and Hoeffding Trees enable immediate detection.
Demirhan, H. (2024)[24]	Accuracy 99%, Sensitivity and Specificity 0.90+, MCC 0.80+.	Real-time implementable online fuzzy framework.
Abd-Ellatif, L. et al. (2025)[25]	Accuracy (94–99%), Precision (>95%), Recall (90–97%), F1-Score (~0.95), AUC-ROC (>0.98), lower false positive rate (-40%), latency <100 ms per transaction, near real-time detection.	ATAD-Net, FraudX AI, and GNN+Autoencoder combine hybrid approaches with human and automatic verification.
Theodorakopoulos, L. et al. (2025)[26]	Accuracy 95–99%, Precision >95%, Recall 90–98%, F1 ~0.96, ROC-AUC >0.98, reduction of false positives, low latency (<100 ms), efficiency in distributed processing.	XGBoost and CatBoost with PySpark enable real-time detection and monitoring.
El-Kenawy, E.-S. M. et al. (2024)[27]	Accuracy 99.39%, F1-score 0.9939, high Recall and AUC > 0.99.	RNN and LSTM enable real-time detection with low computational cost.
Rawashdeh, E. (2024)[28]	Evaluates with G-Mean, Recall, and AUC, demonstrating high accuracy and low false positive rate.	Automatic detection in near real time thanks to the optimization of weights and neurons in the model.
Alarfaj, F. K. & Shahzadi, S. (2025)[29]	Accuracy 94–99%, Precision >95%, Recall 90–97%, F1 ~0.95, AUC-ROC >0.98, -40% false positives.	LSTM, CNN, Autoencoders, graphs, federated for continuous real-time monitoring.
Wang, H. (2024)[30]	Accuracy, Precision, Recall, F1, AUC/AUPRC, latency (s), throughput (TPS), MCC.	Online models: Hoeffding Trees, incremental RF/XGBoost, optimized RNN/LSTM, streaming and federated GNN.
Saha, S. C. (2024)[31]	Accuracy: 94–99%, Precision: 90–>95%, Recall: 90–98%, F1-Score: 0.9–0.96, AUC-ROC: 0.68–>0.98, MCC, FPR, latency <100 ms, false positive reduction ~40%	LSTM, CNN, Autoencoders, hybrid models (ML+DL), Graph Neural Networks, Ensemble ML (Random Forest + Logistic Regression + AdaBoost), FinGraphFL.
Baisholan, N. et al. (2025)[32]	Accuracy (94–99%), Precision (>95%), Recall (90–97%), F1-Score (~0.95), AUC-ROC (>0.98), lower false positive rate (-40%), latency <100 ms, near real-time detection.	LSTM, CNN, Autoencoders, hybrid ML+DL models, and federated approaches such as FinGraphFL, which enable adaptive learning and online processing.
Brown, J. (2022)[33]	Metrics such as Accuracy (90–99%), Precision, Recall, F1-score, and AUC-ROC are reported, in addition to a low false positive rate and high early detection.	Online models such as Adaptive Random Forest, Online SVM, Streaming Autoencoders, and Graph Neural Networks enable immediate detection and continuous monitoring in real time.
Al-Maari, A. A. et al. (2025)[34]	Accuracy 95–99%, Precision >95%, Recall 90–98%, F1 ~0.96, AUC >0.98, with ~40% fewer false positives, demonstrating high efficiency and reliability.	LSTM, CNN, and hybrid models facilitate online detection and continuous monitoring with adaptive learning.

Kcennedy, R. K. L. et al. (2024)[35]	Accuracy, Precision, Recall, F1, ROC-AUC, AUPRC, MCC, FP rate, inference time (ms). E.g.: DL studies report F1/AUC ~0.98–0.999 in controlled datasets; AUPRC improves with synthesized labels.	LSTM, CNN, and hybrid models facilitate online detection and continuous monitoring with adaptive learning.
Ibomoiye, D. M., et al. (2024)[36]	AUC (~99% with GAN-GRU), Sensitivity 0.992, Specificity 1.000, Very high accuracy (~99%), High F1 score, Low false positive rate.	GAN + RNN/LSTM/GRU enables continuous training and adaptation
Tayebi, M. et al. (2025)[37]	Accuracy, Precision, Recall, F1-score, ROC-AUC, AUPRC, MCC, FPs rate, inference time (ms), throughput (tx/s). Typical values in studies: AUC/F1 ≈ 0.90–0.999 in controlled datasets.	XGBoost/LightGBM (lightweight), Logistic, Random Forest pruned, Hoeffding Trees (streaming). Possible with optimization: LSTM/CNN pruned, lightweight Autoencoders. More costly: GNN/Transformers (require infrastructure optimization).
Cascavilla, G. (2025)[38]	AUC (~68–85% depending on model and dataset), TP Rate (varies by model: IsolationForest 41–59% Merchants; Autoencoder ~77–85% in some scenarios), High accuracy (~90% due to imbalance), Low/modest F1 due to class rarity.	Lightweight models per cardholder (IF, OCSVM) and optimized AE architectures enable near-online detection; more expensive assemblies require optimization.
AbouGrad, H. (2025)[39]	ROC–AUC: 66.20%, PR-AUC: 1.24%, Precision 99%, Recall showed lower coverage, F1-Score: ~98% between precision and recall, TPR remains high in regions with low false positive rates	Lightweight local models (classifiers or AEs) enable online detection at each node; periodic aggregation supports near-continuous monitoring.
Liu, J. (2025)[40]	accuracy 99.21%, precision 97.92%, recall 96.15% , F1-score 97.03% y AUC 99.31%	The CCNN is efficient and can be integrated into near-real-time pipelines; it requires optimized inference for low latency.
Ullah, H. (2022)[41]	Accuracy: 99.9 % Precision: 93 % F1-score: 85.71 % AUC: 98 %	The study suggests that CNN models can be applied in online transaction contexts.
Yu, J. (2024)[42]	The hybrid model showed Recall 94.85%, F1 ≈ 93.4%, AUC > 0.97, and a +10.7% improvement in recall; MCC and BCR exceeded baselines, confirming reliability and early detection.	LightGBM/XGBoost with fast extraction allows
Sun, Y. (2023)[43]	GRU 95.2/96.0/0.95, LSTM 94.0/97.1/0.94, MLP 92.8/95.2/0.93, AdaBoost 96.6/98.4/0.97, RF 94.5/96.1/0.94	LSTM/GRU LightGBM/XGBoost or lightweight hybrid models.
Al Balawi, S. (2023)[44]	Precisión: 83% Recall: 84% Overall accuracy: 99.81% F1-score: 83.72% Loss: 0.00244	CNN 1-D using CPU/GPU in appropriate infrastructure.
Alsagri, H. S. (2025)[45]	Precisión: 99.5% Recall (Early detection): 90.1% F1-score: > 90% Accuracy: approx. 99% Model cost: 0.421 F1-score DNN: 87% F1-score Random Forest: 84% F1-score SVM: 82%	Multi-stage architecture with fast sorters and DNN enables online scoring
Akour, I. (2025)[46]	Precision 90.51%, Recall 90%, F1-score 89.88%, Accuracy 99.93%, AUC 98%, and Recall CNN–Attention 93.28%	The hybrid requires intensive training, but its inference is fast for online scoring; it is recommended in real systems with adequate infrastructure, taking care with the generation of synthetic samples.
Benchaji, I. (2021)[47]	The metrics obtained include AUC: ~99.5% effective classification capacity MAE: error ≈ 0.6% MSE: error ≈ 0.3% Fraud detected: in a highly unbalanced dataset (only 1.2% were fraud)	The LSTM model enables real-time, online detection.
Owoh, N. (2024)[48]	The reported metrics include accuracy (99.97%), precision (99.91%), recall (99.89%), F1-score (99.89%), and AUC (0.999), demonstrating an excellent balance between sensitivity and specificity.	The proposed ensemble model enables immediate and continuous fraud detection in real time, making it suitable for online banking systems and automated transaction monitoring applications.
Strelcenia, E. (2023)[49]	It was evaluated using Precision, Recall, F1, Accuracy, and ROC; K-CGAN combined with XGBoost and MLP achieved 1.0 in Precision, Recall, and F1 in several cases, perfectly classifying the test set.	XGBoost, RF, and MLP are suitable for immediate detection in online pipelines; K-CGAN reinforces training for continuous monitoring systems.
Ren, J. (2024)[50]	Stacking Ensemble = Precision 99.35 Accuracy 99.42 F1-Score 99.36 Recall 99.38 AUC 99.50	The Stacking Ensemble model
Fedushko, S. (2023)[51]	The reported metrics include AUC (≈94.6% for Logistic Regression, ≈95.4% for stacking) and F1-score (0.96), demonstrating high reliability.	The study does not explicitly test online detection or continuous real-time monitoring.

Plakandaras, V. (2022)[52]	Accuracy = 99.9 % AUC-ROC = 98.1 % Precision = 79.6 % Recall (fraud detection) = 84.8 % F1-Score = 82.1 % Balanced Accuracy = 92.4 % Specificity = 99.9 %	JAD enables immediate retraining and application of the model in card issuers, making it practical for rapid updates.
Alatawi, M. N. (2025)[53]	RF: Prec 100.0%, Acc 99.999%, F1 99.99%, Recall 99.99%, AUC 99.99% GBM: Prec 99.95%, Acc 99.986%, F1 99.92%, Recall 99.90%, AUC 99.98%	The combination of ML/DL with cloud/big data enables real-time detection.
Muduli, D. (2025)[54]	(Stacking Ensemble): Accuracy: 99.95% Precision: 99.93% Recall (Sensibilidad): 99.97% F1-score: 99.95% AUC: 1.00 FPR (False Positive Rate): 0.02% (the lowest among the models compared).	The pipeline inference is lightweight and suitable for real-time use, with scalable architecture, and stacking requires adaptations for continuous learning in streaming.
Feng X et al (2024)[55]	Accuracy, Precision, Recall, F1-score, and training time.	Optimized SVM and RF/GBDT enable real-time deployment; CDL streamlines updates.

Fig. 2 details the citations of references used, identifying the sources with the greatest impact that form the basis of the field of study. The analysis reveals that the work of Abd-Ellatif, L. et al. is the most influential, with 129 citations. This is followed in importance by the references of Sun, Yanxia, with 100 citations and Adejo, J. et al., with 92 citations. The prominence of this small group of authors indicates that current research relies heavily on a core of consolidated knowledge, which guides the methodologies and direction of analysis on fraud detection.

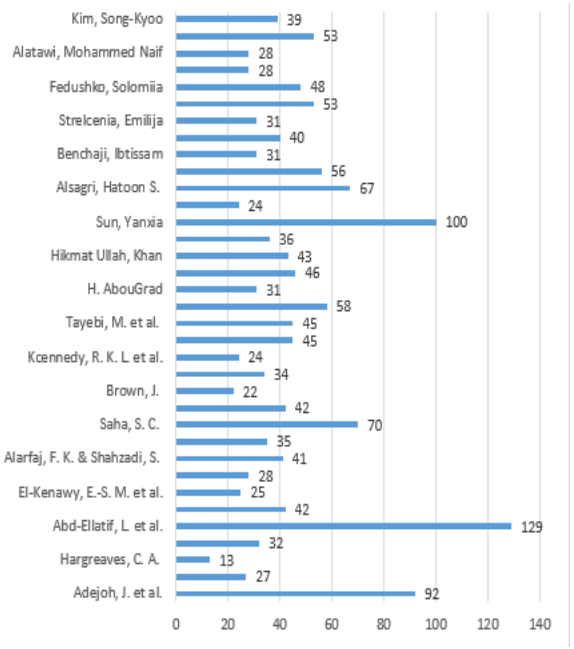

Fig. 2. References used.

C. Word Cloud

Fig. 3 shows the most frequent words identified by Bibliometrix, among which the following stand out: machine learning, deep learning, fraud detection, credit cards, artificial intelligence, cybersecurity, random forest, support vector machines, logistic regression, federated learning, and generative adversarial networks. These words reflect the focus of research on the use of advanced artificial intelligence techniques for financial fraud detection.

Fig. 3. Word cloud.

D. Three-Field Diagram

Fig. 4 presents the three-field diagram, which visualizes the bibliometric connections between the authors' country of origin (AU_CO), research topics or keywords (ID), and authors (AU). The thicker lines show that countries such as the United States, China, and India are the main centers of scientific production in this field, with a predominant focus on credit card fraud detection through the intensive use of advanced artificial intelligence techniques, such as machine learning and deep learning. This pattern reflects a global trend toward the application of sophisticated algorithms to strengthen cybersecurity and optimize fraud detection systems.

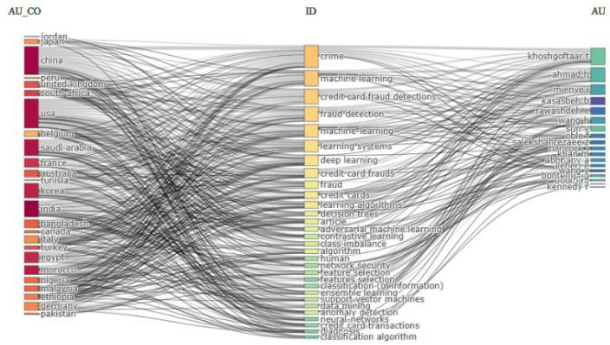

Fig. 4. Three-field diagram.

E. Co-occurrence Network

Fig. 5 presents the co-occurrence network of the most frequent terms in the study area, illustrating the conceptual structure of the research using a map of nodes and links. Key concepts such as machine learning, fraud detection, deep learning, and credit card fraud detection are the most prominent, identified by their larger nodes. These terms act as conceptual nuclei, positioned centrally on the map and serving as connection points for a wide range of interrelated secondary topics. The term crime also stands out as an important and connected concept. The different color-coded clusters (orange, blue, green, red) visually group distinct but related areas of research, where physical proximity between terms indicates a greater strength of thematic co-occurrence.

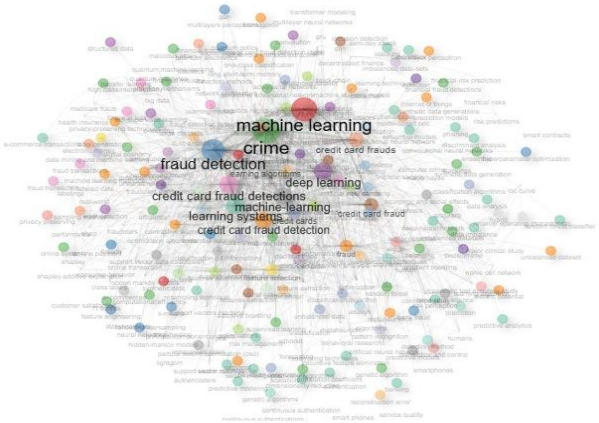

Fig. 5. Co-occurrence network.

F. Factorial Analysis

Fig. 6 shows the thematic grouping according to keyword affinity. There is a concentration in the upper right quadrant with terms such as classification, random forest, credit card fraud, and machine learning, focused on credit card fraud detection. In the upper left quadrant, terms related to fraud detection and algorithm appear, while a small group in green is separated. This confirms that the field focuses on the use of advanced techniques for financial protection.

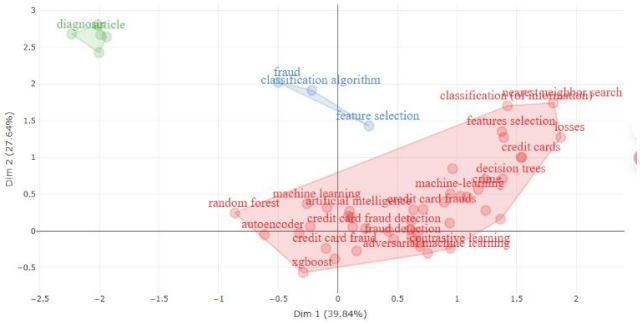

Fig. 6. Factorial analysis.

IV. Discussion

The objective of this review was to identify, analyze, and classify the most effective artificial intelligence models for the early detection of banking fraud in real-time. The findings confirm that deep learning-based approaches perform better than traditional methods, particularly those capable of modeling dependencies in transactional data. In this regard, architectures such as RNN, LSTM, and GRU stand out for their high predictive power, achieving an accuracy of 99.39%, an F1-score of 0.9939, and an AUC greater than 0.99.

These values exceed those reported in previous studies such as that of Sun et al. [43], which shows a significant improvement over previous research. This difference can be explained by the performance achieved by modern models such as LSTM, CNN, and XGBoost, whose accuracy (94–99%), together with other metrics such as Recall, Precision, F1-score, and AUC-ROC, show high effectiveness in fraud detection [22]. Consistently, various authors report high values above 99% for accuracy and AUC, confirming the high sensitivity and specificity of these models in identifying fraudulent transactions [27] , [40].

Similarly, hybrid models that combine traditional techniques such as XGBoost, Random Forest, or Logistic Regression with deep or generative architectures significantly increase the robustness of the system. These methods leverage the representational power of deep networks, achieving outstanding performance in imbalanced contexts [37], [48], [49]. In line with the above, the results obtained are consistent with those reported by authors who have evaluated advanced models for fraud detection. Khan et al. highlight that current classification models allow complex patterns to be captured with greater accuracy than traditional methods, which coincides with the performance observed in the LSTM, RNN, and CNN models analyzed in this review [56]. Muaz et al. specify that the effectiveness of the system necessarily depends on the proper handling of both imbalance and preprocessing, reinforcing the idea that data quality is an important factor in improving model performance, including Deep Learning models [57].

On the other hand, Chergui et al. suggest that semi-supervised methods can be combined with advanced classification methods to better adjust to frequent changes in the types of financial fraud. This shows the importance of using models capable of learning sequences and dynamic variations that arise in fraud behavior [58]. Finally, Aghware et al. emphasize in their research that hybrid strategies combining deep techniques with clustering or assembly methods increase the robustness of the system, supporting the results of this review on the good performance of combined models [59]. Overall, the evidence reviewed shows that deep learning models and hybrid approaches currently represent the most effective and reliable solutions for detecting banking fraud, thus surpassing traditional methods.

V. Conclusion

The objective of this review was to identify, analyze, and classify the most effective artificial intelligence models for the early detection of banking fraud in real-time, especially in an environment where transactions are increasingly fast and changing.

Based on the study conducted, it can be concluded that the ML and DL models most commonly used in the detection of fraudulent transactions are Random Forest (RF), which is one of the most accurate and widely used ML models, followed by

XGBoost, considered one of the most accurate and widely used supervised learning approaches, Support Vector Machine (SVM) in third place, and Short-Term Memory Networks (LSTM), which are a type of deep architecture, and Graph-based Approaches (GNN), which allow for the integration of temporal, relational, and behavioral patterns, in fourth place.

Deep learning architectures, described by deep learning (DL) models, have proven to be particularly effective at capturing temporal and multivariate patterns, improving the accuracy and scalability of systems. First and foremost are Recurrent Neural Networks (RNN), LSTM, and GRU, which are essential for capturing the temporal dynamics of fraud. secondly, Convolutional Neural Networks (CNN), which are also used to capture complex patterns, and Autoencoders (AE), which are often used for anomaly detection, as unsupervised models are useful for identifying hidden patterns and irregular behaviors in large volumes of data, achieving an accuracy of 99.39%, an F1-score of 0.9939, and an AUC greater than 0.99.

Within hybrid and ensemble models, the combination of different algorithms or the integration of multiple approaches is considered a robust strategy that improves fraud detection, such as models that combine classical techniques, such as XGBoost or Random Forest, with deep architectures, achieving near-perfect performance, registering F1-scores and AUC between 0.98 and 1.00. Banking fraud solutions applied by other researchers have implemented and evaluated a wide range of Machine Learning (ML) and Deep Learning (DL) models, often outperforming traditional methods such as Random Forest, XGBoost, and short- and long-term memory networks (LSTM) used for fraud detection.

However, the study has some limitations related to the differences between the approaches used in the empirical works reviewed, the variety of databases used, and the frequent use of public datasets that do not always represent the complexity that exists in real banking systems. Finally, it is recommended that future research test these models in real operating environments, with real-time data, unified metrics, and scenarios where new types of fraud appear. In addition, it would be valuable to explore more efficient hybrid techniques and methods, such as federated learning, which could improve the adaptability of systems and strengthen their ability to detect early fraud.

REFERENCES

[1] C. Ikeda, K. Ouazzane, Q. Yu, and S. Hubenova, "New Feature Engineering Framework for Deep Learning in Financial Fraud Detection," International Journal of Advanced Computer Science and Applications, vol. 12, no. 12, pp. 10–21, 2021, doi: 10.14569/IJACSA.2021.0121202.

[2] B. Mytnyk, O. Tkachyk, N. Shakhovska, S. Fedushko, and Y. Syerov, "Application of Artificial Intelligence for Fraudulent Banking Operations Recognition," Big Data and Cognitive Computing 2023, Vol. 7, Page 93, vol. 7, no. 2, p. 93, May 2023, doi: 10.3390/BDCC7020093.

[3] L. Hernandez Aros, L. X. Bustamante Molano, F. Gutierrez-Portela, J. J. Moreno Hernandez, and M. S. Rodríguez Barrero, "Financial fraud detection through the application of machine learning techniques: a literature review," Humanit Soc Sci Commun, vol. 11, no. 1, pp. 1–22, Dec. 2024, doi: 10.1057/S41599-024-03606-0;SUBJMETA.

[4] N. Husnaningtyas and T. Dewayanto, "FINANCIAL FRAUD DETECTION AND MACHINE LEARNING ALGORITHM (UNSUPERVISED LEARNING): SYSTEMATIC LITERATURE REVIEW," Jurnal Riset Akuntansi Dan Bisnis Airlangga, vol. 8, no. 2, pp. 1521–1542, Nov. 2023, doi: 10.20473/JRABA.V8I2.49927.

[5] Y. Yanto, L. Lisah, and R. Tandra, "The Best Machine Learning Model for Fraud Detection In Banking Sector: A Systematic Literature Review," eCo-Buss, vol. 7, no. 2, pp. 1361–1384, Dec. 2024, doi: 10.32877/EB.V7I2.1474.

[6] H. Abbassi, S. El Mendili, and Y. Gahi, "Real-Time Online Banking Fraud Detection Model by Unsupervised Learning Fusion," HighTech and Innovation Journal, vol. 5, no. 1, pp. 185–199, Mar. 2024, doi: 10.28991/HIJ-2024-05-01-014.

[7] S. M. N. Nobel et al., "Unmasking Banking Fraud: Unleashing the Power of Machine Learning and Explainable AI (XAI) on Imbalanced Data," Information 2024, Vol. 15, Page 298, vol. 15, no. 6, p. 298, May 2024, doi: 10.3390/INFO15060298.

[8] F. Li and Z. Chen, "Dynamic quantification anti-fraud machine learning model for real-time transaction fraud detection in banking," Discover Computing, vol. 28, no. 1, pp. 1–15, Dec. 2025, doi: 10.1007/S10791-025-09549-7/TABLES/5.

[9] S. Xiang et al., "Semi-supervised Credit Card Fraud Detection via Attribute-Driven Graph Representation," Proceedings of the 37th AAAI Conference on Artificial Intelligence, AAAI 2023, vol. 37, pp. 14557–14565, Dec. 2024, doi: 10.1609/aaai.v37i12.26702.

[10] C. Wang, C. Nie, and Y. Liu, "Evaluating Supervised Learning Models for Fraud Detection: A Comparative Study of Classical and Deep Architectures on Imbalanced Transaction Data," May 2025, doi: 10.48550/arXiv.2505.22521.

[11] M. R. Baker, Z. N. Mahmood, and E. H. Shaker, "Ensemble Learning with Supervised Machine Learning Models to Predict Credit Card Fraud Transactions," Revue d'Intelligence Artificielle, vol. 36, no. 4, pp. 509–518, Aug. 2022, doi: 10.18280/RIA.360401.

[12] D. Wang et al., "A Semi-supervised Graph Attentive Network for Financial Fraud Detection," Proceedings - IEEE International Conference on Data Mining, ICDM, vol. 2019-November, pp. 598–607, Feb. 2020, doi: 10.1109/ICDM.2019.00070.

[13] M. Ben Boubker, T. Elmettat, A. Eddaoui, and S. Ouahabi, "Fraud Detection in Financial Transactions Using Machine Learning with Oversampling Techniques: A Case Study of a Moroccan Bank," Journal of Electrical Systems, vol. 20, no. 10s, pp. 6443–6448, Jul. 2024, Accessed: Sep. 26, 2025. [Online]. Available: https://journal.esrgroups.org/jes/article/view/6664

[14] G. Zioviris, K. Kolomvatsos, and G. Stamoulis, "An intelligent sequential fraud detection model based on deep learning," Journal of Supercomputing, vol. 80, no. 10, pp. 14824–14847, Jul. 2024, doi: 10.1007/S11227-024-06030-Y/TABLES/4.

[15] M. J. Page et al., "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," BMJ, vol. 372, Mar. 2021, doi: 10.1136/BMJ.N71.

[16] D. Moher et al., "Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement," PLoS Med, vol. 6, no. 7, p. e1000097, Jul. 2009, doi: 10.1371/JOURNAL.PMED.1000097.

[17] A. Shukla and T. Kashni, "Análisis bibliométrico de la literatura sobre fraudes y estafas bancarias," Revista de Delitos, vol. 32, no. 3, pp. 729–750, Mar. 2025, doi: 10.1108/JFC-08-2024-0252.

[18] J. V. Raúl, A. A. Laberiano, M. V. Pedro, and Y. A. Cesar, "Revolución financiera: un análisis sistémico de la inteligencia artificial y el aprendizaje automático en el sector bancario," Revista Internacional de Ingeniería Eléctrica e Informática, vol. 14, no. 1, pp. 1079–1090, Feb. 2024, doi: 10.11591/ijece.v14i1.pp1079-1090.

[19] O. A. Oke and N. Cavus, "El papel de la IA en los servicios financieros: un análisis bibliométrico," Journal of Computer Information Systems, vol. 65, no. 4, pp. 518–530, 2025, doi: 10.1080/08874417.2024.2304545.

[20] A. S. Gangwar, A. Shukla, M. Sharma, and A. Kumar, "Un análisis bibliométrico exhaustivo del lavado de dinero y estafas relacionadas: tendencias, influencias y lagunas en la investigación," Revista Internacional de Investigación de Ámbito Multidisciplinario, vol. 6, no. 3, pp. 1236–1251, Jul. 2025, doi: 10.47857/irjms.2025.v06i03.04926.

[21] J. Adejoh, N. Owoh, M. Ashawa, S. Hosseinzadeh, A. Shahrabi, and S. Mohamed, "An Adaptive Unsupervised Learning Approach for Credit

Card Fraud Detection," Big Data and Cognitive Computing, vol. 9, no. 9, Sep. 2025, doi: 10.3390/bdcc9090217.

[22] I. Y. Hafez, A. Y. Hafez, A. Saleh, A. A. Abd El-Mageed, and A. A. Abohany, "A systematic review of AI-enhanced techniques in credit card fraud detection," J Big Data, vol. 12, no. 1, Dec. 2025, doi: 10.1186/s40537-024-01048-8.

[23] S. Ma and C. A. Hargreaves, "Addressing Credit Card Fraud Detection Challenges with Adversarial Autoencoders," Big Data and Cognitive Computing, vol. 9, no. 7, Jul. 2025, doi: 10.3390/bdcc9070168.

[24] G. Charizanos, H. Demirhan, and D. İçen, "An online fuzzy fraud detection framework for credit card transactions," Expert Syst Appl, vol. 252, Oct. 2024, doi: 10.1016/j.eswa.2024.124127.

[25] L. Abd-Ellatif, M. Abrar, and A. A. K. Ismaeel, "ATAD-Net: An Adaptive Deep Learning Framework for Real-Time Financial Fraud Detection," Advances in Artificial Intelligence and Machine Learning, vol. 5, no. 2, pp. 3988–4003, 2025, doi: 10.54364/AAIML.2025.52225.

[26] L. Theodorakopoulos, A. Theodoropoulou, A. Tsimakis, and C. Halkiopoulos, "Big Data-Driven Distributed Machine Learning for Scalable Credit Card Fraud Detection Using PySpark, XGBoost, and CatBoost," Electronics (Switzerland), vol. 14, no. 9, May 2025, doi: 10.3390/electronics14091754.

[27] E. S. M. El-Kenawy et al., "Credit Card Fraud Detection based on Deep Learning Models," Mesopotamian Journal of Computer Science, vol. 2024, pp. 204–213, Dec. 2024, doi: 10.58496/MJCSC/2024/016.

[28] E. Rawashdeh, N. Al-Ramahi, H. Ahmad, and R. Zaghloul, "Efficient credit card fraud detection using evolutionary hybrid feature selection and random weight networks," International Journal of Data and Network Science, vol. 8, no. 1, pp. 463–472, Dec. 2024, doi: 10.5267/j.ijdns.2023.9.009.

[29] F. Khaled Alarfaj and S. Shahzadi, "Enhancing Fraud Detection in Banking with Deep Learning: Graph Neural Networks and Autoencoders for Real-Time Credit Card Fraud Prevention," IEEE Access, vol. 13, pp. 20633–20646, 2025, doi: 10.1109/ACCESS.2024.3466288.

[30] H. Wang, Q. Liang, J. T. Hancock, and T. M. Khoshgoftaar, "Feature selection strategies: a comparative analysis of SHAP-value and importance-based methods," J Big Data, vol. 11, no. 1, Dec. 2024, doi: 10.1186/s40537-024-00905-w.

[31] Z. Xia and S. C. Saha, "FinGraphFL: Financial Graph-Based Federated Learning for Enhanced Credit Card Fraud Detection," Mathematics, vol. 13, no. 9, May 2025, doi: 10.3390/math13091396.

[32] N. Baisholan, J. E. Dietz, S. Gnatyuk, M. Turdalyuly, E. T. Matson, and K. Baisholanova, "FraudX AI: An Interpretable Machine Learning Framework for Credit Card Fraud Detection on Imbalanced Datasets," Computers, vol. 14, no. 4, Apr. 2025, doi: 10.3390/computers14040120.

[33] M. N. Vadlamudi, S. Doma, S. Fouzia Sayeedunnisa, M. Hijab, R. M. Chinnem, and B. Sankara Babu, "Towards Transparent Fraud Detection: Explainable AI and Multi-algorithm Optimization in Financial Security," International Journal of Intelligent Engineering and Systems, vol. 18, no. 10, pp. 698–712, Nov. 2025, doi: 10.22266/ijies2025.1130.45.

[34] A. A. Al-Maari, M. Abdulnabi, Y. Nathan, A. Ali, U. Ali, and M. Khan, "Optimized Credit Card Fraud Detection Leveraging Ensemble Machine Learning Methods," Engineering, Technology and Applied Science Research, vol. 15, no. 3, pp. 22287–22294, Jun. 2025, doi: 10.48084/etasr.10287.

[35] R. K. L. Kennedy, F. Villanustre, T. M. Khoshgoftaar, and Z. Salekshahrezaee, "Synthesizing class labels for highly imbalanced credit card fraud detection data," J Big Data, vol. 11, no. 1, Dec. 2024, doi: 10.1186/s40537-024-00897-7.

[36] I. D. Mienye and T. G. Swart, "A Hybrid Deep Learning Approach with Generative Adversarial Network for Credit Card Fraud Detection," Technologies (Basel), vol. 12, no. 10, Oct. 2024, doi: 10.3390/technologies12100186.

[37] M. Tayebi and S. El Kafhali, "A novel approach based on XGBoost classifier and Bayesian optimization for credit card fraud detection," Cyber Security and Applications, vol. 3, Dec. 2025, doi: 10.1016/j.csa.2025.100093.

[38] E. Karnavou, G. Cascavilla, G. Marcelino, and Z. Geradts, "I know you're a fraud: Uncovering illicit activity in a Greek bank transactions with unsupervised learning," Expert Syst Appl, vol. 288, Sep. 2025, doi: 10.1016/j.eswa.2025.128148.

[39] H. AbouGrad and L. Sankuru, "Online Banking Fraud Detection Model: Decentralized Machine Learning Framework to Enhance Effectiveness and Compliance with Data Privacy Regulations," Mathematics, vol. 13, no. 13, Jul. 2025, doi: 10.3390/math13132110.

[40] Y. Wu et al., "A Deep Learning Method of Credit Card Fraud Detection Based on Continuous-Coupled Neural Networks," Mathematics 2025, Vol. 13, vol. 13, no. 5, Feb. 2025, doi: 10.3390/MATH13050819.

[41] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, "Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms," IEEE Access, vol. 10, pp. 39700–39715, 2022, doi: 10.1109/ACCESS.2022.3166891.

[42] L. Ding, L. Liu, Y. Wang, P. Shi, and J. Yu, "An AutoEncoder enhanced light gradient boosting machine method for credit card fraud detection," PeerJ Comput Sci, vol. 10, p. e2323, Oct. 2024, doi: 10.7717/PEERJ-CS.2323.

[43] I. D. Mienye and Y. Sun, "A Deep Learning Ensemble With Data Resampling for Credit Card Fraud Detection," IEEE Access, vol. 11, pp. 30628–30638, 2023, doi: 10.1109/ACCESS.2023.3262020.

[44] S. Al Balawi and N. Aljohani, "Credit-card Fraud Detection System using Neural Networks," International Arab Journal of Information Technology, vol. 20, no. 2, pp. 234–241, Mar. 2023, doi: 10.34028/iajit/20/2/10.

[45] H. S. Alsagri, "Hybrid Machine Learning-Based Multi-Stage Framework for Detection of Credit Card Anomalies and Fraud," IEEE Access, vol. 13, pp. 77039–77048, 2025, doi: 10.1109/ACCESS.2025.3565612.

[46] I. Akour, N. Mohamed, and S. Salloum, "Hybrid CNN-LSTM With Attention Mechanism for Robust Credit Card Fraud Detection," IEEE Access, vol. 13, pp. 114056–114068, 2025, doi: 10.1109/ACCESS.2025.3583253.

[47] I. Benchaji, S. Douzi, and B. El Ouahidi, "Credit card fraud detection model based on LSTM recurrent neural networks," Journal of Advances in Information Technology, vol. 12, no. 2, pp. 113–118, May 2021, doi: 10.12720/JAIT.12.2.113-118.

[48] A. R. Khalid et al., "Enhancing Credit Card Fraud Detection: An Ensemble Machine Learning Approach," Big Data and Cognitive Computing 2024, Vol. 8, vol. 8, no. 1, Jan. 2024, doi: 10.3390/BDCC8010006.

[49] E. Strelcenia, S. Prakoonwit, E. Strelcenia, and S. Prakoonwit, "Improving Classification Performance in Credit Card Fraud Detection by Using New Data Augmentation," AI 2023, Vol. 4, Pages 172-198, vol. 4, no. 1, pp. 172–198, Jan. 2023, doi: 10.3390/AI4010008.

[50] S. Zhu et al., "A Financial Fraud Prediction Framework Based on Stacking Ensemble Learning," Systems 2024, Vol. 12, vol. 12, no. 12, Dec. 2024, doi: 10.3390/SYSTEMS12120588.

[51] B. Mytnyk et al., "Application of Artificial Intelligence for Fraudulent Banking Operations Recognition," Big Data and Cognitive Computing 2023, Vol. 7, vol. 7, no. 2, May 2023, doi: 10.3390/BDCC7020093.

[52] V. Plakandaras, P. Gogas, T. Papadimitriou, and I. Tsamardinos, "Credit Card Fraud Detection with Automated Machine Learning Systems," Applied Artificial Intelligence, vol. 36, no. 1, Dec. 2022, doi: 10.1080/08839514.2022.2086354;WGROUP:STRING:PUBLICATION.

[53] M. N. Alatawi, "Detection of fraud in IoT based credit card collected dataset using machine learning," Machine Learning with Applications, vol. 19, p. 100603, Mar. 2025, doi: 10.1016/J.MLWA.2024.100603.

[54] R. K. Gupta et al., "Enhanced framework for credit card fraud detection using robust feature selection and a stacking ensemble model approach," Results in Engineering, vol. 26, p. 105084, Jun. 2025, doi: 10.1016/J.RINENG.2025.105084.

[55] X. Feng, S.-K. Kim, X. Feng, and S.-K. Kim, "Novel Machine Learning Based Credit Card Fraud Detection Systems," Mathematics 2024, Vol. 12, vol. 12, no. 12, Jun. 2024, doi: 10.3390/MATH12121869.

[56] S. Khan, A. Alourani, B. Mishra, A. Ali, and M. Kamal, "Developing a Credit Card Fraud Detection Model using Machine Learning Approaches," International Journal of Advanced Computer Science and Applications, vol. 13, no. 3, pp. 411–418, Mar. 2022, doi: 10.14569/IJACSA.2022.0130350.

[57] A. Muaz, M. Jayabalan, and V. Thiruchelvam, "A Comparison of Data Sampling Techniques for Credit Card Fraud Detection," IJACSA) International Journal of Advanced Computer Science and Applications, vol. 11, no. 6, 2020, Accessed: Nov. 16, 2025. [Online]. Available: www.ijacsa.thesai.org

[58] C. Hamza, A. Lylia, C. Nadine, and C. Nicolas, "Semi-supervised Method to Detect Fraudulent Transactions and Identify Fraud Types while Minimizing Mounting Costs," IJACSA) International Journal of Advanced Computer Science and Applications, vol. 14, no. 2, p. 2023, Accessed: Nov. 16, 2025. [Online]. Available: https://www.kaggle.com/mlg-ulb/creditcardfraud

[59] F. O. Aghware, R. E. Yoro, P. O. Ejeh, C. C. Odiakaose, F. U. Emordi, and A. A. Ojugo, "DeLClustE: Protecting Users from Credit-Card Fraud Transaction via the Deep-Learning Cluster Ensemble," IJACSA) International Journal of Advanced Computer Science and Applications, vol. 14, no. 6, p. 2023, Accessed: Nov. 16, 2025. [Online]. Available: www.ijacsa.thesai.org