Vol.7, No.2, Desember 2024
Available online at: https://jurnal.kdi.or.id/index.php/eb

The Best Machine Learning for Fraud Detection in Banking Sector: A Systematic Literature Review

Yanto[1)*], Lisah[2)], Re'gina Tandra[3)]

[1)]Khettasoft@gmail.com

[1)]Universitas Buddhi Dharma
Jl.Imam Bonjol No. 41 RT.002/RW003 Karawaci, Kec. Karawaci, Kota Tangerng Banten 15115

Jejak Artikel:

Upload: 30 Oktober 2024
Revisi: 07 Desember 2024
Diterima: 10 Desember 2024
Tersedia online: 12 Desember 2024

Keywords:

machine learning;
fraud detection;
banking;
systematic literature review;
fraud prevention;

ABSTRACT

In today's financial sector, institutions are facing increasing threats from sophisticated fraud schemes, driven by rapid technological advancements and the growing reliance on digital transactions, a trend further exacerbated by the COVID-19 pandemic. This systematic literature review (SLR) examines 81 scholarly articles from 2014 to 2024, focusing on the use of machine learning (ML) algorithms for fraud detection in banking. Drawing on data from Dimensions.ai and a combination of public and proprietary financial datasets, the review evaluates the performance of various fraud detection techniques. In 2023, global financial losses due to fraud exceeded $34 billion, highlighting the critical need for more advanced fraud detection systems. The review finds that hybrid models consistently deliver the highest accuracy rates, with a notable 99.38% accuracy. These models outperform others in key performance metrics and are particularly effective at detecting a broader range of financial crimes, as evidenced by a study conducted by five major Japanese financial institutions. While traditional methods remain useful in specific contexts, advanced hybrid models offer superior precision and resilience. Future research should focus on refining hybrid models and integrating real-time data streams to enhance fraud detection in the rapidly evolving.

INTRODUCTION

The financial industry, particularly the banking sector, has witnessed a significant rise in fraudulent activities, fueled by the rapid pace of technological advancement and the increasing reliance on digital transactions. This surge has been exacerbated by the COVID-19 pandemic, which accelerated the shift to online banking, consequently expanding the opportunities for fraudsters to exploit.

[*] Corresponding author

EISSN. 2622-4305
PISSN. 2622-4291
Published by Komunitas Dosen Indonesia.
DOI: 10.32877/eb.v7i2.1474

As highlighted in the Nilson Report (Outseer, 2023), the global financial industry faced losses surpassing $34 billion in 2023 as a result of fraud, emphasizing the critical need for strong and effective detection systems.

Machine learning (ML) has emerged as an indispensable tool for detecting and mitigating fraud in the banking industry. A variety of ML models have been developed and deployed to identify fraudulent activities with remarkable precision and effectiveness. This systematic literature review (SLR) aims to explore and identify the most optimal ML models for fraud detectionng in the banking sector, focusing on open-access publications published between 2014 and 2024.

Several studies have utilized algorithm model to detect credit card fraud, achieving notable accuracy and demonstrating the effectiveness of these classical models in identifying fraudulent transactions. However, as fraud schemes became increasingly complex, more advanced models began to outperform these traditional approaches in terms of performance..

(Sudhakar & Kaliyamurthie, 2023), as well as (Rahmatullah et al., 2022), Other studies utilized XGBoost, which consistently exhibited exceptional performance, delivering high accuracy and precision in detecting credit card fraud. Its capacity to manage large datasets and its resilience to overfitting have made XGBoost a preferred model for fraud detection (Kumar et al., 2024) and (Parmar et al., 2020) One study examined the effectiveness of K-Nearest Neighbors (KNN), concluding that it is a dependable model with strong performance in identifying various forms of banking fraud. Similarly, (Lin, 2023) and (Kolodiziev et al., 2020) Another study emphasized the benefits of LightGBM, noting its ability to deliver high accuracy across a range of financial contexts.

Random Forest, another popular ML model, was extensively studied by (D. Shah & Sharma, 2023) and (Abdul Salam et al., 2024)research demonstrated that Random Forest could attain high accuracy rates, establishing it as a reliable model for detecting both credit card and bank transaction fraud.

Autoencoders have also been used effectively for fraud detection. (Mitra et al., 2022) and (Almuteer et al., 2021) demonstrated the high accuracy of autoencoders in identifying fraudulent credit card transactions. Meanwhile, Support Vector Machine (SVM) was employed by (Sasikala et al., 2022)) and (Chile et al., 2021), proving effective in detecting both bank and credit card fraud.

(Mohmad, 2022) and (ismael, 2024) explored Bidirectional LSTM, showing that It can attain remarkable accuracy in identifying credit card fraud by recognizing sequential patterns within transaction data. Additionally, Generative Adversarial Networks (GANs) were used by (Ali et al., 2024), achieving high accuracy in credit card fraud detection by generating realistic fraudulent examples to train detection models.

(Du et al., 2024) A novel hybrid model, integrating AE-XGB-SMOTE-CGAN, was introduced, achieving outstanding accuracy and top scores in metrics such as MCC, TNR, and ACC. This hybrid approach capitalizes on the strengths of multiple techniques, improving detection rates while minimizing false positives.

The literature consistently indicates that advanced models, such as XGBoost, hybrid methods, and deep learning techniques, generally outperform traditional models in fraud detection. However, simpler models like Naive Bayes and Logistic Regression still hold value, owing to their simplicity and effectiveness in specific situations. Hybrid models, which combine multiple advanced techniques, it has been demonstrated to improve forecasting accuracy by harnessing the combined strengths of individual methods.(Ampountolas, 2023)

According to (Thilakaratne et al., 2019), The first step in conducting a systematic literature review is to Develop pertinent research questions that are specific, clear, and provide a clear direction for the study. In this context, we have formulated the following three research questions (RQs) based on our predetermined topic:

RQ1: Which machine learning models have demonstrated the highest effectiveness in detecting fraud within the banking sector?

RQ2: What types of datasets are most frequently used, and how do they impact the performance of the models?

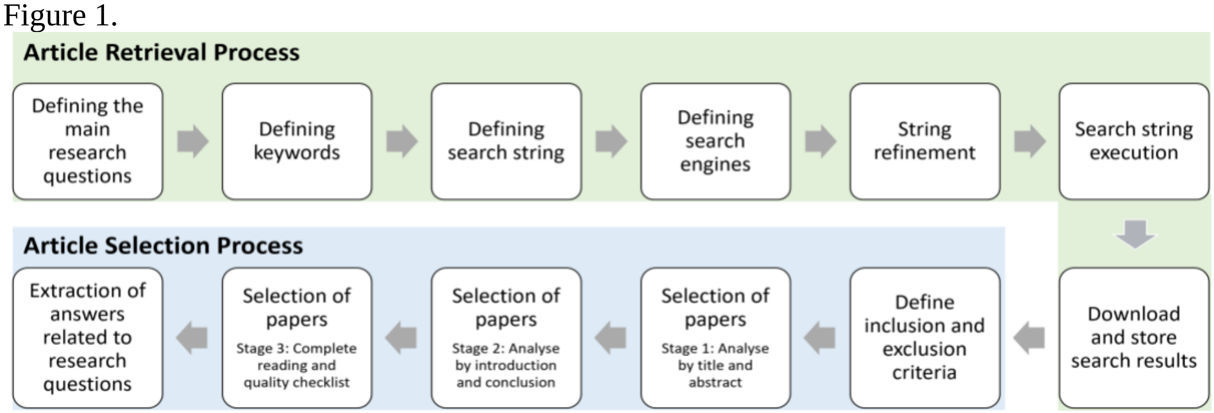
RQ3: What are the average accuracy rates achieved by these models?

RQ4: What types of fraud are most frequently detected using these models?

This review will provide a comprehensive overview of the current landscape of ML-based fraud detection in the banking sector, offering valuable insights into the most effective models and methodologies. By addressing these research questions, we aim to contribute to the development of more robust and efficient fraud detection systems, ultimately enhancing the security and integrity of the financial sector.

RESEARCH METHOD

This comprehensive literature review aims to evaluate the most effective algorithm models for fraud detection in banking, focusing on their accuracy, scalability, interpretability, and robustness. The following models are highlighted through a comparative analysis based on performance accuracy. The methodology is structured around several key phases: formulating precise research questions, identifying relevant concepts and keywords, constructing the search query, selecting appropriate search engines, refining the query, executing the search, analyzing the search results, establishing inclusion and exclusion criteria, choosing pertinent studies, and extracting insights to answer the research questions. This SLR approach ensures a thorough, reliable, and unbiased assessment of the studies, providing a solid foundation for drawing conclusions and making recommendations. In accordance with the methodology outlined by (Al-Sabaeei et al., 2023), this research adopted the SLR steps in (Thilakaratne et al., 2019) To conduct the systematic literature review (SLR), one must adhere to the key steps outlined in Figure 1.



Source: Thilakaratne et al., 2019

Figure 1 - Systematic literature review process

1. Determining relevant concepts and keyword

In the second stage, We identified three key concepts essential to the topic and research questions:

Keyword 1: "Machine Learning model"
Keyword 2: "Fraud Detection"
Keyword 3: "Banking Sector"
By contemplating synonyms, orthographic variants, and abbreviations, we extrapolated the ensuing lexicon: "Machine Learning models," "Machine Learning model," "Fraud Detection," "fraud detection," "Banking Sector," and "Banking."

2. Constructing the search query

The ascertained keywords were subsequently amalgamated through the use of Boolean operators. By employing the PICO and "Medical Subject Headings" (MESH) frameworks, the ensuing search string was contrived: "Machine Learning model" OR "Machine Learning models" AND "Fraud Detection" OR "fraud detection" AND "Banking Sector" OR "Banking."

"Machine Learning model" OR "Machine Learning models" AND "Fraud Detection" OR "fraud detection" AND "Banking Sector" OR "Banking"

3. Selecting suitable search engines

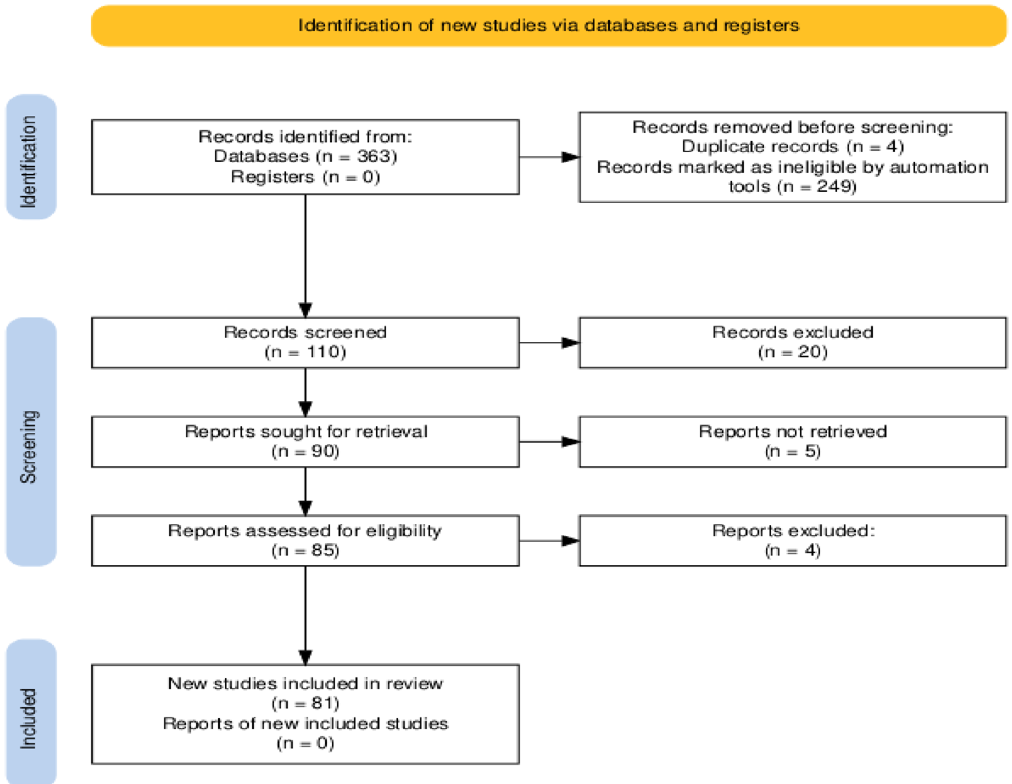
In this phase, We chose relevant search engines to ensure comprehensive coverage of the literature, thereby enhancing the likelihood of discovering highly relevant articles. For this review, Dimensions.ai was chosen as the primary database.

4. Refining the query

The search string was trialed in the Dimensions.ai database to evaluate the pertinence of the returned articles. Pre-identified relevant papers, which could serve as potential primary studies, were located. In instances where no pertinent results emerged, the search string was modified and fine-tuned accordingly to enhance its effectiveness.

5. Executing the search and reviewing the search results

Upon finalizing the search string, it was executed in the Dimensions.ai database, yielding 363 publications. The results of the search process are visually represented in the PRISMA flow diagram, illustrated in Figure 2.



Source: Author, 2024

Figure 2 - PRISMA diagram flow

6. Defining inclusion and exclusion criteria

We focused on ensuring the selection of relevant and high-quality studies based on several inclusion criteria: the publication year was between 2014 and 2024, the articles were open access (All OA), the publication type was an article, and the articles were written in English. The exclusion criteria were as follows: articles not related to the banking sector, articles that did not use machine learning for fraud detection, and non-research articles, such as editorials, opinion pieces, and reviews without empirical data.

7. Choosing relevant studies

The initial search yielded 81 articles, which were then screened for relevance by reviewing their titles, abstracts, and keywords. Articles that did not meet the inclusion criteria were excluded. The remaining articles were subjected to a detailed full-text review to ensure they fulfilled all specified criteria. This meticulous screening process ultimately resulted in 81 articles being included in the final analysis.

8. Extracting answers to the research questions.

The research questions were addressed through a systematic analysis of the papers selected in the previous step. A spreadsheet was employed to document the potential answers as each paper was reviewed. A summary of the data collected during the final screening phase is presented in Table 1, while the detailed findings and interpretations are discussed in the subsequent Findings and Discussion section.

Table 1. Literature Review Article List

No	Author(s)/ Year	ML Model	Dataset	Type of Fraud	Results	Conclusion
1	(Can et al., 2020)	Naive Bayes and Logistic Regression	35 Turkish banks transaction	Credit Card Fraud	Naive Bayes scored 100% accuracy	Naïve Bayes is highly effective.
2	(Sudhakar & Kaliyamurthie, 2023)	Various Model	1,048,575 transactions of European Bank in 2013	Credit Card Fraud	XG Boost accuracy 99.96%,	XG boost provided better accuracy
3	(Du et al., 2024)	Hybrid Model	284,807 transactions in European Bank in 2013	Credit Card Fraud	Hybrid accuracy 99.93%,	Hybrid had the highest accuracy values
4	(M. N. K. Kumar et al., 2024)	K-Nearest Neighbors (KNN)	Data fraud prevention market size in 2016–2022	Online Banking Fraud	K-Nearest Neighbors (KNN) 97.74%	KNN is highly performance
5	(Adeyemo & Obafemi, 2024)	Machine Learning Algorithms	57 sample ML is enhancing fraud prevention in Nigeria Banks	Online Banking Fraud	82% respondent agree ML effective for fraud detection	Machine learning algorithms effective for Fraud Prevention
6	(Alunowska Figueroa et al., 2021)	Various Model	4 million cyber crime in Mexico Bank	Financial Banking Fraud	TMS has high accuracy	TMS effective for financial fraud prevention
7	(Suri* et al., 2020)	Decision Tree	UCI ML repository (age, job, education, etc.)	Online Banking Fraud	Decision Tree Accuracy 77.96%	Decision Tree Effective to predict fraud
8	(Sultana et al., 2023)	ST-BPNN	284,807 transactions in European Bank in 2013	Credit Card Fraud	ST-BPNN F1 Score 92,2%, AUC-ROC 100%	ST-BPNN Model Effective to predict credit card fraud
9	(Lin, 2023)	Light BM	Payments accounts and credit card transactions by Kaggle	Online Banking Fraud	Light GBM model showed high accuracy	Light GBM is ideal for fraud detection
10	(Sasikala et al., 2022)	Various Model	Personal identity, credit card number, CVV,(OTP) and PIN	Credit Card Fraud	SVM Precision 98.78%	SVM is affective to detect credit card fraud
11	(Ore-Areche et al., 2022)	Various Model	284,807 transactions in European Bank	Credit Card Fraud	Isolation forest accuracy 99.74%	SILOF is effective for credit card fraud detect
12	(Togbe et al., 2021)	Various Model	Shuttle, SMTP) and SEA.	Online Bankin	Isolated Forest ASD F1 81%	Isolated Forest ASD is detector data anomalies

				g Fraud		
13	(Mytnyk et al., 2023)	Various Model	284,807 transactions that occurred in two day and data kaggle	Online Bankin g Fraud	Logistic regression accuracy 94.6%	Logistic regression is effective to detect transaction bank Fraud
14	(Zareapoor & Shamsolmoali , 2015)	Various Model	100,000 records of e-commerce transactions.	Credit Card Fraud	decision tree the highest accuracy 80%	Decision tree Effective to cathing credit card Fraud
15	(Du et al., 2023)	Hybrid Auto Encoder Light BM	284,807 transactions in European Bank	Credit Card Fraud	Hybrid accuracy 99.95%	Hybrid is more suitable for detecting fraud
16	(González-Carrasco et al., 2019)	Bayes Network	126 scenario experiments	Online Bankin g Fraud	Bayes Network accuracy 99.90%	Bayes Network is best choice to detect bank transaction
17	(Kolodiziev et al., 2020)	Light BM	A technical minimum of information about transactions	Online Bankin g Fraud	Light GBM accuracy 99.94%	Light BM is Effective to detect Illegal Transaction
18	(Asomura et al., 2023)	Various Model	forecasting foreign exchange rates	Online Bankin g Fraud	Various Model accuracy 99.80%	Various Model suitable detect Banking Fraud
19	(Prof. Antara Bhattacharya et al., 2023)	Artificial Neural Networks (ANN)	Loan Amount Requested, Loan Term	Bank Loan Fraud	ANN accuracy 82%	ANN is Effective for Detect Bank Loan Fraud
20	(Arora et al., 2023)	Various Model	credit card bank transaction in ecommerce in India	Credit Card Fraud	Logistic Regression precision 80%	Logistic regression is the best for credit card fraud detection.
21	(A. Shah & Mehta, 2021)	Various Model	284,807 transactions in European Bank in 2013	Credit Card Fraud	Random Forest accuracy 96.4%	Random Forest is better to detect fraud
22	(T. Patil & Khadare, 2023)	Random Forest	customers bank data	Credit Card Fraud	Random Forest Acc 99.78%	Random Forest is best to detect fraud
23	(Parmar et al., 2020)	K-Nearest Neighbors (KNN)	284,807 credit card transactions in EU Bank	Credit Card Fraud	K-Nearest Neighbors (KNN) accuracy 99.95%	K-Nearest Neighbors (KNN) is effective to hanf
24	(Mitra et al., 2022)	Autoenco der	284,807 credit card transactions in EU Bank	Credit Card Fraud	Auto Encoder accuracy 97%	autoencoder is highest accuracy to detect credit card fraud
25	(D. Shah & Sharma, 2023)	Decision Tree,	Data kaggle simulated credit card transaction	Credit Card Fraud	Random Forest precision 98.43%	Random Forest is accurate for detect fraud

26	(Mohmad, 2022)	Random Forest Bidirectional LSTM	ATM transactions in (Europay-MasterCard-Visa)	Credit Card Fraud	Bidirectional LSTM accuracy 82.4%	Bidirectional LSTM is is better for detect fraud
27	(P. S. G. Kumar et al., 2019)	Various Model	Transactions using credit cards .	Credit Card Fraud	the optimal accuracy for logistic regression	Logistic regression is effective to detect credit card Fraud
28	(Joshi et al., 2020)	SMOTE	The Keggle credit card transaction	Credit Card Fraud	SMOTE accuracy 98.7%	SMOTE will finding credit card fraud
29	(Charan et al., 2022)	Logistic Regression	The Keggle credit card transaction	Credit Card Fraud	Logistic Regression accuracy 98%	Logistic Regression is effective to detect fraud
30	(Zhan2023)	Various Model	Credit card holder data	Credit Card Fraud	Logistic regression is highest accurcy	Logistic Regression is effective to detect fraud
31	(Ponaganti, 2019)	Various Model	credit card transactions and build up a predictive model based on the dataset	Credit Card Fraud	Logistic Regression sesitivity 83%	Logistic Regression is effective to detect credit card fraud
32	(Dr. P. Siva Kumar, 2020)	Random Forest	13 billion master card transactions in India	Credit Card Fraud	Random Forest accuracy 99.8%	Random Forest is effective to detect fraud
33	(ismael, 2024)	bidirectional long-short term memory (BiLSTM)	customers behavior and models	Credit Card Fraud	BiLSTM accuracy 98%	BiLSTM highest accuracy to detect fraud
34	(Li et al., 2022)	Various Hybrid Model	284,807 credit card transactions in European Bank	Credit Card Fraud	Hybrid precision 99.99%	Hybrid is best model for credit card fraud detection
35	(Narsimha et al., 2022)	Various Model	leverage e-currency exchanges and other financial transaction	Financial Banking Fraud	Random Forest accuracy 82.94 %	Random Forest is better model to detect financial Fraud
36	(Jayanthi et al., 2023)	Various Hybrid Model	two-day credit card transaction details of people from Europe in kaggle	Credit Card Fraud	CCLR and CCRF accuracy 99.96%	Hybrid CCLR dan CCRF is the best model to detect credit card
37	(Haddab, 2023)	Various Model	274,807 credit card transactions in European bank	Online Banking Fraud	Random Forest accurcy 93.96%	Random Forest is better detect banking fraud
38	(Almuteer et al., 2021)	Various Model	284315 imbalanced credit card transaction	Credit Card Fraud	The Autoencoder	AE is the best model to detect

					accuracy of 99%	fraud in credit card
39	(Shmatko et al., 2021)	Random Forest	Credit Card Transaction	Credit Card Fraud	Random Forest accuracy 77%	Random Forest is better to detect credit card fraud
40	(Ojulari et al., 2024)	H2O autoencoder deep learning models	1.2 million transaction records from 10 Nigerian bank's ATM	Online Banking Fraud	H2O autoencoder accuracy 97.60%	H2O autoencoder deep learning models is the best model to detect ATM Fraud
41	(Chile et al., 2021)	SVM and Random Forest	set of URLs containing benign and phishing URLs a	Phishing Banking Fraud	Random Forest accuracy 85.6%	Random Forest is much more scurto detect phishing site
42	(T et al., 2022)	Random Forest, SVM and Decision Tree	284,807 credit card transactions in EU Bank in European Bank	Credit Card Fraud	Random Forest accuracy 97.6%	Random Forest was Develped to detect the fraud in credit card
43	(Rahmatullah et al., 2022)	Various Model	283,823 credit card transaction downloaded from kaggle	Credit Card Fraud	XGBoost scenario obtained 99% accu	XGBoost is the best model to detect credit card fraud
44	(Bandyopadhyay, 2020)	Stacked-RNN Model	6362620 transaction during COVID-19 from Kaggle	Online Banking Fraud	Stacked-RNN accuracy 99.87%	Stacked-RNN is the best model to detect bank transactions fraud
45	(ÇELİK & GEZER, 2022)	Various Model	13077 Malware is marked by WEKA software	Online Banking Fraud	Random Tree accuracy 83%	Random tree is better model for trickbot and emotet Banking Detection
46	(Almhaithawi et al., 2020)	Various Model	284,807 to 568,630 with 284,315 fraud sample instead of 492 collect from Kaggle	Credit Card Fraud	CB+SMOTE+BMR 97.62%	CB+SMOTE+BMR is better model to detect credit card fraud
47	(Abdul Salam et al., 2024)	Various Model	284,807 transactions in European Bank in 2013	Credit Card Fraud	Random Forest accuracy 99.99%	random forest is highly accuracy to detect credit card fraud
48	(Usman et al., 2024)	Various Model	demographic, behavioral, risk, and transactional form BAF	Financial Banking Fraud	KNN accuracy 98.84%	KNN is highly performance
49	(Fritz-Morgenthal et al., 2022)	Various Model	Based on the discussions at the Round Table AI at Firm	Financial Banking Fraud	-	in AI systems used for financial risk manaement

50	(Ojugo et al., 2023)	Various Hybrid Model	57,345-transaction (cardholder data, bank name and others)	Online Banking Fraud	2-hidden layer neural network accurcy 99%	2-hidden layer neural network is effective to detect Bank Fraud
51	(Nageswara Rao Moparthi, 2024)	Various Model	Bank transaction from kaggle.com	Online Banking Fraud	-	LightGBM, The accuracy of the scam detection
52	(Kawade et al., 2022)	Various Model	284,807 transactions in European Bank in 2013	Credit Card Fraud	Isolated Forest has accuracy 95.76%	Isolated Forest is the best to detect credit card fraud
53	(Paladini et al., 2023)	Various Model	transactions having the same IP, Session ID, and ASN_CC	Online Banking Fraud	XGBoost obtained accuracy 94.30%	XGBoost is effective model to detect bank transaction fraud
54	(Waykar, 2023)	Various Model	Account No, transaction average, per day from Kaggle	Credit Card Fraud	Isolation Forest model has accuracy 94%	Isolation Forest model is highly accuracy to detect fraud
55	(Lokanan & Sharma, 2022)	Various Model	406 cases from the IIROC's website	Financial Banking Fraud	Gridsearch model obtained accuracy 99.5%	Gridsearch Model is effective to predictinvestment fraud
56	(Akinje & Fuad, 2021)	Various Model	6362620 transactions, (cash out, payment, cash in and transfer)	Online Banking Fraud	Gradient Boosting classifiers obtained a 100% accuracy	Gradient Boosting classifiers is effectived to detect Bank Transaction Fraud
57	(Kjamilji & Güney, 2023)	Various Model	credit card information, log data of computer and network systems	Online Banking Fraud	Multinomial Naïve Bayes(MNB) accuracy 99.1%	Multinomial Naïve Bayes(MNB) is effective for banking system secured
58	(Nwachukwu & Boatengu, 2022)	Artificial Neural Network Algorithm	German credit dataset thousands of bank customer information	Online Banking Fraud	ANNAlgortithms accuracy 98%	ANN is effective for indentify customer credit risk
59	(Domashova & Kripak, 2021)	Various Model	typical international transactions on bank cards of individuals	Online Banking Fraud	Adaboost method accuracy 99.99%	Adaboost method is effective for detect bank transaction fraud

60	(Ashwini T G, 2023)	Various Model	Customer data, financial history, credit scores, and behavior are crucial elements	Online Bankin g Fraud	-	AI has positively impacted fraud detection
61	(Ali et al., 2024)	Various Model	284,807 transactions in European Bank in 2013 (data kaggle)	Credit Card Fraud	GAN accuracy 99.9%	GAN a highly accurate for fraud detection
62	(Wang et al., 2022)	Various Model	Israel credit card transactions (non-time series) and a bank loan dataset (time series)	Online Bankin g Fraud	SVM RF-Balance obtained accuracy 98.67%	SVM RF-Balance is best model to solved online Fraud Detection
63	(Venkata Suryanarayan a et al., 2018)	Various Model	100,000 credit card holder data	Credit Card Fraud	Logistic Regression accuracy 96.24%	Logistic Regression is best for detect credit card fraud
64	(Kousika et al., 2021)	Various Model	30 transaction records from Kaggle	Credit Card Fraud	random forest accuracy 94%	random forest is best to detect credit card fraud
65	(Rahangdale et al., 2022)	Various Model	Credit card Identity	Credit Card Fraud	Random Forest accuracy 95.5%	random forest is the best for detect credit card fraud
66	(Vanini et al., 2023)	Various Model	140 million transactions, customer info and activity	Online Bankin g Fraud	-	ML model effective to detect anomalies data
67	(Ileberi et al., 2021)	Various Model	284,808 credit card transactions of an EU financial institution dataset.(Kaggle data)	Credit Card Fraud	AdaBoost-SVM obtained accuraci 99.96%	AdaBoost-SVM is best model for detection credit card fraud
68	(Bharuka et al., 2024)	Various Model	Confidential customer information	Phishin g Bankin g Fraud	XGBoost obtained accuracy 98.4%	XGBoost is the best to detect phishing
69	(S. Patil et al., 2018)	Various Model	day to day and past historical credit card transaction	Credit Card Fraud	Random Forest Decision Tree accuracy 76%	Random Forest Decision Tree is the highest accuracy
70	(Kanamori et al., 2022)	Various Hybrid Model	financial crimes in fives Japan Bank	Online Bankin g Fraud	hybrid model accuracy 94.7%	Hybrid model generated high performance for detecting criminals' bank accounts
71	(Arri, 2022)	Various Model	Credit card transaction fraud	Credit Card Fraud	XG Boost accuracy 99.94%	XG Boost is the best for ccard fraud detection
72	(Xiang et al., 2023)	GTAN (Graph Temporal Attention Network)	FFSD, Yelp Chi graph and Amazon graph dataset	Credit Card Fraud	GTAN accuracy 99.9%	GTAN a accurate for credit card raud detection

73	(Tran et al., 2019)	Graph p Laplacian semi-supervised learning	Dataset from https://www.kaggle.com/mlg-ulb/creditcardfraud	Credit Card Fraud	GpLS - supervised learning accuracy 88.52%	GpLS learning is significan to detect credit card fraud
74	(Rode et al., 2022)	Various Model	on real-world credit card transaction datasets.	Credit Card Fraud	ML model precision 99.6%	MLis effective to detect credit card fraud
75	(Chowdari, 2021)	Various Model	284,807 transactions in European Bank in 2013	Credit Card Fraud	Logistic Regresson accuracy 94.9%	Logistic Regression is credit card fraud detection
76	(Wei, 2023)	Support Vector Machine (SVM)	nearly 80 million credit card fraudulent	Credit Card Fraud	SVM accuracy 96.35%	SVM is affective to detect credit card fraud
77	(Smiles* & Kumar, 2019)	Various Model	This synthetic dataset is the initial dataset produced by Kaggle	Online Bankin g Fraud	Random Forest accuracy 99.99%	Random Forest is the best model to detect online payment fraud
78	(Nesvijevskai a et al., 2021)	Various Model	customer information, several other confidential data	Financi al Bankin g Fraud	Deep Neural Network is highest Accuracy	Deep Neural Network is effective to detect money laundry
79	(Sahu* et al., 2)	Various Model	284,807 transactions in European Bank in 2013	Credit Card Fraud	Logistic Regression accuracy 99%	Logistic Regression is effective to detect credit crad fraud
80	(Caprian & of Moldova, 2023)	Various Model	Data transaction size, location, time, device, purchase data, consumer behavior	Online Bankin g Fraud	-	Machine Learning can predicted combating bank fraud
81	(Gupta et al., 2023)	Various Model	Card Account number, PIN, credit card transaction	Credit Card Fraud	XG Boost acurracy 99% and precision 91%,	XG Boost is the best model for credit card fraud detection

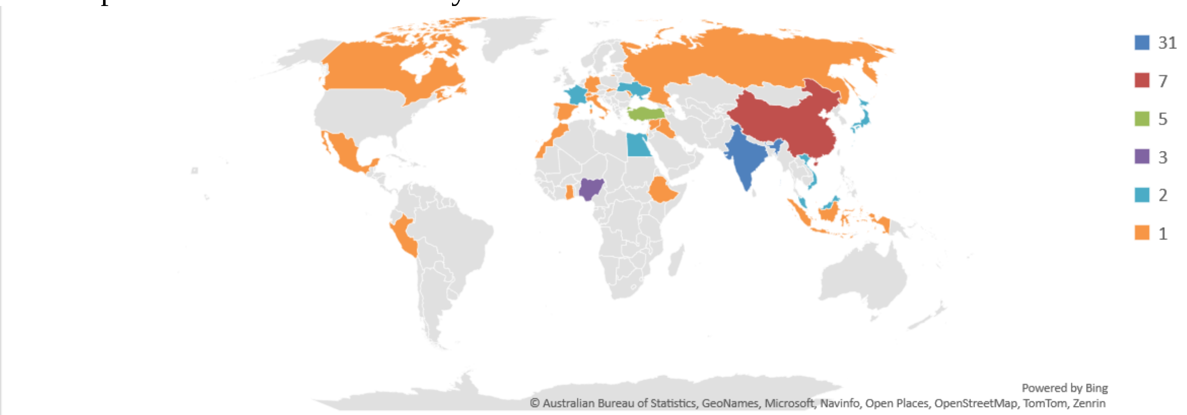
Source: Author, 2024

RESULTS AND DISCUSSION

This section summarizes the findings of the systematic literature review based on 81 articles on machine learning models for banking fraud detection. The results are categorized into geographical distribution, machine learning models, datasets, and types of fraud addressed. **A comparative analysis** is used to evaluate the effectiveness of various algorithms in terms of accuracy, efficiency, and fraud detection across different conditions and datasets.

1. Geographical Distribution of Research

The 81 research articles originate from various countries, with from notable contributions the India, China, Germany, Turkey, Nigeria, Egypt, France, USA, Russia and the Indonesia. The distribution of research by country is illustrated in Figure 3, which shows the number of articles published from each country.



Source: Author, 2024

Figure 3 - Geographical Distribution of Research

2. Machine Learning Models Used for Fraud Detection in the Banking Sector

The first research question (RQ1) sought to identify the machine learning models employed for fraud detection in the banking sector. Table 2 summarizes the findings from the 81 articles reviewed. As illustrated in Table 2 and Figure 4, a total of 27 distinct algorihm models were utilized across 44 different publications.

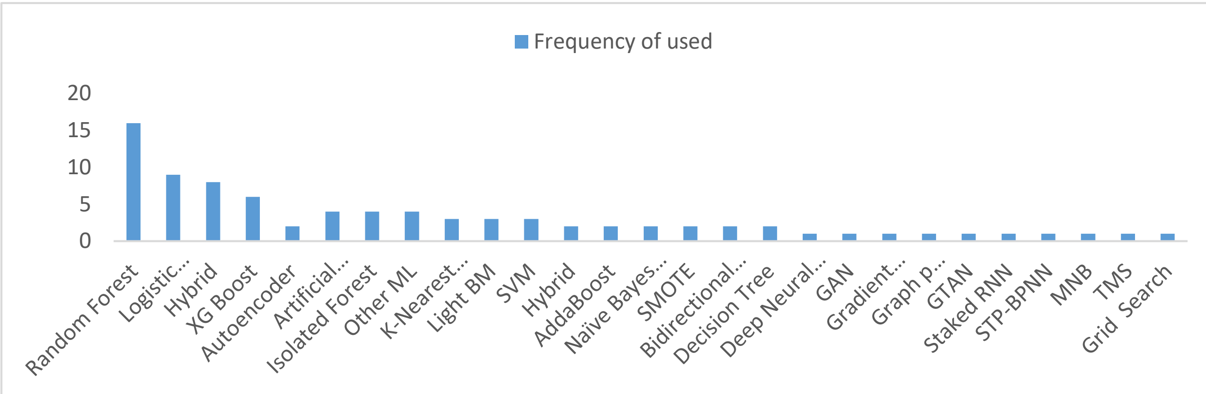
Table 2. Prevalence of Machine Learning Models in Fraud Detection Applications

No.	ML Models	Reference	Usage Frequency
1..	Random Forest	(Abdul Salam et al., 2024; Asomura et al., 2023; ÇELİK & GEZER, 2022; Chile et al., 2021; Dr. P. Siva Kumar, 2020; Haddab, 2023; Kousika et al., 2021; Narsimha et al., 2022; S. Patil et al., 2018; T. Patil & Khadare, 2023; Rahangdale et al., 2022; A. Shah & Mehta, 2021; D. Shah & Sharma, 2023; Shmatko et al., 2021; Smiles* & Kumar, 2019; (T et al., 2022)	**16**
2.	Logistic Regression	(Abdul Salam et al., 2024; Asomura et al., 2023; ÇELİK & GEZER, 2022; Chile et al., 2021; Dr. P. Siva Kumar, 2020; Haddab, 2023; Kousika et al., 2021; Narsimha et al., 2022; S. Patil et al., 2018; T. Patil & Khadare, 2023; Rahangdale et al., 2022; A. Shah & Mehta, 2021; D. Shah & Sharma, 2023; Shmatko et al., 2021; Smiles* & Kumar, 2019; (T et al., 2022)	**9**
3.	Hybrid	(Du et al., 2024); (Du et al., 2023) ; (Ojulari et al., 2024); (Ojugo et al., 2023); (Kanamori et al., 2022); (Almhaithawi et al., 2020); (Jayanthi et al., 2023); (Li et al., 2022)	8

4.	XG Boost	(Sudhakar & Kaliyamurthie, 2023); (Rahmatullah et al., 2022); (Paladini et al., 2023); (Bharuka et al., 2024); (Arri, 2022); (Gupta et al., 2023)	6
5.	Hybrid	(Du et al., 2024); (Du et al., 2023) ; (Ojulari et al., 2024); (Ojugo et al., 2023); (Kanamori et al., 2022); (Almhaithawi et al., 2020); (Jayanthi et al., 2023); (Li et al., 2022)	8
6.	Autoencoder	(Mitra et al., 2022); (Almuteer et al., 2021)	2
7.	Artificial Neural Network	(Prof. Antara Bhattacharya et al., 2023); (Fritz-Morgenthal et al., 2022); (Nwachukwu & Boatengu, 2022); (Ashwini T G, 2023)	4
8.	Isolated Forest	(Ore-Areche et al., 2022); (Togbe et al., 2021); (Kawade et al., 2022); Waykar, 2023)	4
9.	K-Nearest Neighbors (KNN)	(M. N. K. Kumar et al.,2024); (Parmar et al., 2020); (Usman et al., 2024)	3
10.	Light BM	(Lin, 2023); (Kolodiziev et al., 2020);(Nageswara Rao Moparthi, 2024)	3
11.	SVM	(Sasikala et al., 2022); (Wang et al., 2022); (Wei, 2023)	3
12.	AddaBoost	(Domashova & Kripak, 2021); (Ileberi et al., 2021)	2
13.	Bidirectional LSTM	(Mohmad, 2022); (ismael, 2024)	2
14.	Decision Tree	(Suri* et al., 2020); (Zareapoor & Shamsolmoali, 2015)	2
15.	Naïve Bayes Network	(Can et al., 2020); (González-Carrasco et al., 2019)	2
16.	SMOTE	(Joshi et al., 2020)	2
17.	Deep Neural Network	(Nesvijevskaia et al., 2021)	1
18.	GAN	(Ali et al., 2024)	1
19.	Gradient Boosting	(Akinje & Fuad, 2021)	1
20.	Graph p Laplacian semi-supervised learning	(Tran et al., 2019)	1
21.	Grid Search	(Lokanan & Sharma, 2022)	1
22.	GTAN	(Xiang et al., 2023)	1
23.	MNB	(Kjamilji & Güney, 2023)	1
24.	Staked RNN	(Bandyopadhyay, 2020)	1
25.	STP-BPNN	(Sultana et al., 2023)	1
26.	TMS	(Alunowska Figueroa et al., 2021)	1
27.	Other ML	(Adeyemo & Obafemi, 2024); (Vanini et al., 2023); (Rode et al., 2022); (Caprian & of Moldova, 2023)	4

Source: Author, 2024

Table 2 reveals that less frequently used models include Complement Grid Search, TMS, MNB,
STP-BPNN, and Stacked RNN, while Random Forest, Logistic Regression, Hybrid approaches, XGBoost, and Artificial Neural Networks were the most commonly used. Notably,Random Forest was the top model for fraud detection in banking sector.



Source: Author, 2024

Figure 4 – Frequency of Usage Machine Lerning Model for Fraud Detection

3. Common Datasets Used

The second research question (RQ2) aimed to determine the datasets commonly used in these studies, which vary significantly, including both public and proprietary data. Public datasets are often sourced from financial institutions and online repositories such as BAF and Kaggle, while proprietary datasets are typically acquired directly from specific banks or financial services. These datasets play a crucial role in model performance and are summarized in Table 1

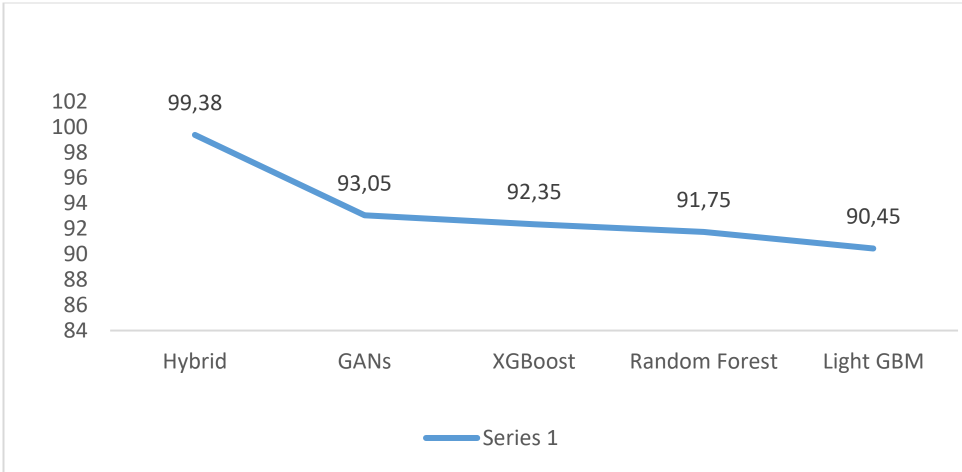
4. The most effective machine learning models for fraud detection in the banking sector.

The third research question (RQ3) sought to identify the most effective machine learning models for fraud detection in banking. To do so, we compared the performance of the five most commonly used models, using accuracy as the key metric. Many studies used a shared dataset, making it feasible to evaluate and compare the models' performances.The results of this analysis are presented in Table 3 and Figure 5, which highlight the relative effectiveness of each model

Table 3: Top 5 ML Model Accuracies for Fraud Detection in Banking Sector

No	Model	Average Accuracy (%)
1	Hybrid	99.38
2	Generative Adversarial Networks (GANs)	93.05
3	XGBoost	92.35
4	Random Forest	91.75
5	Light GBM	90.45

Source: Author, 2024

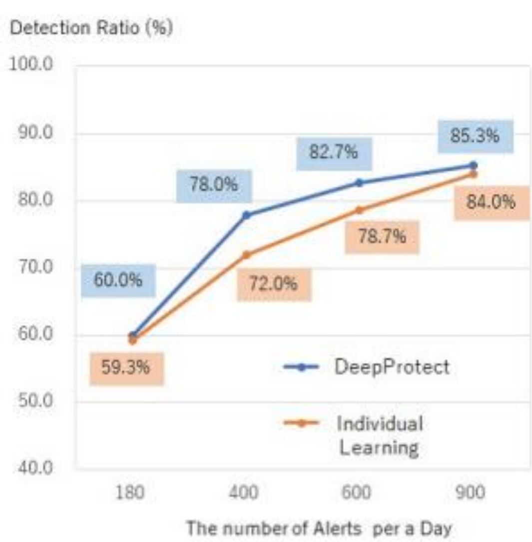


Source: Author, 2024

Figure 5-Top Five Average Accuracies of ML Models for Fraud Detection

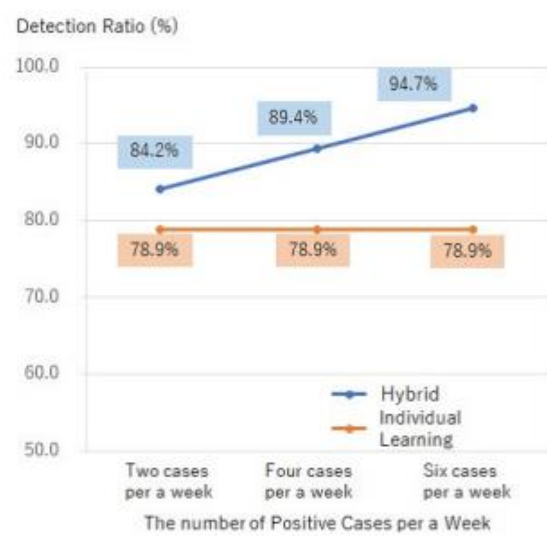
The results presented in Figure 6 show that the LightGBM model performed the least, with an average accuracy of 90.45%. It was followed by Random Forest, XGBoost, GANs, and Hybrid models, which achieved average accuracies of 91.75%, 92.35%, 93.05%, and 99.38%, respectively. The data revealed an interesting contrast: while Random Forest was the most frequently used model (as indicated in Table 2), it ranked fourth in performance, achieving an accuracy of 91.75% (as shown in Figure 5). In contrast, the Hybrid model, which ranked third in terms of usage frequency, outperformed all others with an impressive average accuracy of 99.38%.

A study with five Japanese banks found that hybrid models outperformed individual machine learning models in detecting financial crimes like fraud, money laundering, and unauthorized transfers, demonstrating their superior accuracy and adaptability. (Kanamori et al., 2022)



Source: Kanamori , 2022

Figure 6 - Comparative Detection Fraud Ratio between Deep Learning vs Individual Learning



Source: Kanamori , 2022

Figure 7 - Comparative Detection Fraud Ratio between Hybrid Model vs Individual Model

4. Common Types of Fraud

Research question four (RQ4) explored the most common types of fraud detection in banking. Analysis of 81 articles revealed that Credit Card Fraud was the most frequently studied, addressed in 46 articles.

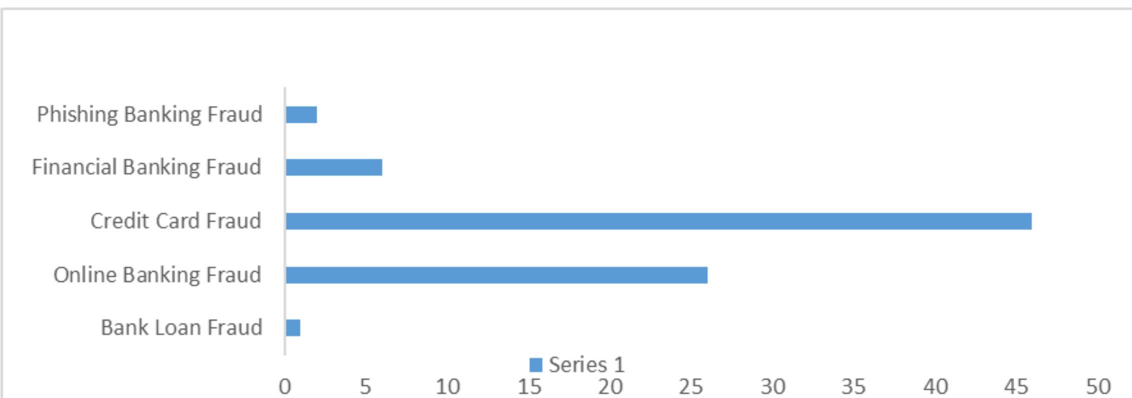
a. **Online Banking Fraud**: Analyzed in 26 articles.
b. **Financial Banking Fraud**: Explored in 6 articles.
c. **Phishing Banking Fraud**: investigated in 2 articles.
d. **Bank Loan Fraud**: Covered in 1 articles(1.24%).

Thus, credit card fraud stands as the most prevalent type of fraud detection in the banking sector. The results are summarized in Figure 8 and Table 4.

Table 4 Common Type of Fraud Detection in Banking Sector

Type of Fraud	Number of dcArticles	%
Credit Card Fraud	46	56.79%
Online Banking Fraud	26	32.09%
Financial Banking Fraud	6	7.41%
Phishing Banking Fraud	2	2.47%
Bank Loan Fraud	1	1.24%

Source: Author, 2024



Source: (Author, 2024)

Figure 8. Common Type of Fraud Detection in Banking Sector

CONCLUSION

The study revealed that credit card fraud is the most prevalent type of financial fraud in the banking sector, constituting 56.79% of cases. It identified 27 different machine learning models utilized for fraud detection, with Random Forest being the most frequently employed, followed by Logistic Regression and Hybrid models. However, the study also found that the most commonly used models do not necessarily deliver the best performance. Despite Random Forest's widespread use, it ranked fourth in performance, achieving an accuracy of 91.75%. In contrast, the Hybrid model, although ranked third in usage, achieved the highest accuracy of 99.38%.

RECOMMENDATIONS

This review underscores the growing importance of hybrid models in fraud detection and suggests that future research should focus on incorporating additional performance metrics such as recall and precision. While traditional models remain effective, deep learning and hybrid approaches demonstrate superior performance. As fraud tactics evolve, banks must invest in cutting-edge machine learning technologies and continuously update their fraud detection systems to stay ahead of emerging threats.

REFERENCES

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

Adeyemo, K., & Obafemi, F. J. (2024). A Survey on the Role of Technological Innovation in Nigerian Deposit Money Bank Fraud Prevention. *South Asian Journal of Social Studies and Economics*, *21*(3), 133–150. https://doi.org/10.9734/sajsse/2024/v21i3790

Akinje, A. O., & Fuad, A. (2021). Fraudulent Detection Model Using Machine Learning Techniques for Unstructured Supplementary Service Data. *International Journal of Innovative Computing*, *11*(2), 51–60. https://doi.org/10.11113/ijic.v11n2.299

Ali, N. T., Hasan, S. J., Ghandour, A., & Al-Hchimy, Z. S. (2024). Improving credit card fraud detection using machine learning and GAN technology. *BIO Web of Conferences*, *97*, 76. https://doi.org/10.1051/bioconf/20249700076

Almhaithawi, D., Jafar, A., & Aljnidi, M. (2020). Example-dependent cost-sensitive credit cards fraud detection using SMOTE and Bayes minimum risk. *SN Applied Sciences*, *2*(9), 1574. https://doi.org/10.1007/s42452-020-03375-w

Almuteer, A. H., Aloufi, A. A., Alrashidi, W. O., Alshobaili, J. F., & Ibrahim, D. M. (2021). Detecting Credit Card Fraud using Machine Learning. *International Journal of Interactive Mobile Technologies (IJIM)*, *15*(24), 108–122. https://doi.org/10.3991/ijim.v15i24.27355

Al-Sabaeei, A. M., Alhussian, H., Abdulkadir, S. J., & Jagadeesh, A. (2023). Prediction of oil and gas pipeline failures through machine learning approaches: A systematic review. In *Energy Reports* (Vol. 10, pp. 1313–1338). Elsevier Ltd. https://doi.org/10.1016/j.egyr.2023.08.009

Alunowska Figueroa, M., Turner-Szymkiewicz, D., Lopez-Rojas, E. A., Cárdenas-Rodriguez, J. S., & Norinder, U. (2021). An approach to benchmark fraud detection algorithms in the COVID-19 era. *Revista Latinoamericana de Economía y Sociedad Digital*, *2*. https://doi.org/10.53857/rpgd2470

Ampountolas, A. (2023). Comparative Analysis of Machine Learning, Hybrid, and Deep Learning Forecasting Models: Evidence from European Financial Markets and Bitcoins. *Forecasting*, *5*(2), 472–486. https://doi.org/10.3390/forecast5020026

Arora, K., Pathak, S., & Dieu Linh, N. T. (2023). Comparative Analysis ofK-Nn, Naïve Bayes, and logistic regression for credit card fraud detection. *Ingenieria Solidaria*, *19*(3), 1–22. https://doi.org/10.16925/2357-6014.2023.03.05

Arri, H. S. (2022). Real-Time Credit Card Fraud Detection Using Machine Learning. *International Journal Of Scientific Research In Engineering And Management*, *06*(04). https://doi.org/10.55041/ijsrem12659

Ashwini T G, M. A. Khan. N. A. H. (2023). Impact of Artificial Intelligence in Banking Sector. *REST Journal on Banking, Accounting and Business*, *2*(3), 51–55. https://doi.org/10.46632/jbab/2/3/7

Asomura, I., Iijima, R., & Mori, T. (2023). Automating the Detection of Fraudulent Activities in Online Banking Service. *Journal of Information Processing*, *31*(0), 643–653. https://doi.org/10.2197/ipsjjip.31.643

Bandyopadhyay, S. K. (2020). Detection of Fraud Transactions Using Recurrent Neural Network during COVID-19. *Journal of Advanced Research in Medical Science & Technology*, *07*(03), 16–21. https://doi.org/10.24321/2394.6539.202012

Bharuka, V., Almeida, A., & Patil, S. (2024). Phishing Detection Using Machine Learning Algorithm. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *10*(2), 343–349. https://doi.org/10.32628/cseit2410228

Can, B., Yavuz, A. G., Karsligil, E. M., & Guvensan, M. A. (2020). A Closer Look Into the Characteristics of Fraudulent Card Transactions. *IEEE Access*, *8*, 166095–166109. https://doi.org/10.1109/access.2020.3022315

Caprian, I., & of Moldova, U. (2023). The Use of Machine Learning for the Purpose of Combating Bank Fraud. *Business Inform*, *7*(546), 140–145. https://doi.org/10.32983/2222-4459-2023-7-140-145

ÇELİK, R., & GEZER, A. (2022). Detection of Trickbot and Emotet Banking Trojans with Machine Learning. *Balkan Journal of Electrical and Computer Engineering*, *10*(4), 377–387. https://doi.org/10.17694/bajece.1031021

Charan, R., Devi, K. K., Teja, G. S., Siddhartha, G. S., & Sitharam, D. (2022). Credit Card Fraud Detection Using Ml Algorithms. *International Journal of Advanced Research in Science, Communication and Technology*, 285–289. https://doi.org/10.48175/ijarsct-7636

Chile, A., Jadhav, M., Thakare, S., & Chavan, Prof. Y. (2021). Detecting Phishing Website Using Machine Learning. *International Journal of Advanced Research in Science, Communication and Technology*, 16–19. https://doi.org/10.48175/ijarsct-1082

Chowdari, G. B. (2021). Supervised Machine Learning Algorithms For Detecting Credit Card Fraud. *EPRA International Journal of Research & Development (IJRD)*, 131–134. https://doi.org/10.36713/epra7636

Domashova, J., & Kripak, E. (2021). Identification of non-typical international transactions on bank cards of individuals using machine learning methods. *Procedia Computer Science*, *190*, 178–183. https://doi.org/10.1016/j.procs.2021.06.023

Dr. P. Siva Kumar, P. S. S. V. (2020). Credit Card Fraudulent Detection Using Machine Learning Algorithm. *International Journal for Research in Engineering Application & Management*, 445–449. https://doi.org/10.35291/2454-9150.2020.0330

Du, H., Lv, L., Guo, A., & Wang, H. (2023). AutoEncoder and LightGBM for Credit Card Fraud Detection Problems. *Symmetry*, *15*(4), 870. https://doi.org/10.3390/sym15040870

Du, H., Lv, L., Wang, H., & Guo, A. (2024). A novel method for detecting credit card fraud problems. *PLOS ONE*, *19*(3), e0294537. https://doi.org/10.1371/journal.pone.0294537

Fritz-Morgenthal, S., Hein, B., & Papenbrock, J. (2022). Financial Risk Management and Explainable, Trustworthy, Responsible AI. *Frontiers in Artificial Intelligence*, *5*, 779799. https://doi.org/10.3389/frai.2022.779799

González-Carrasco, I., Jiménez-Márquez, J. L., López-Cuadrado, J. L., & Ruiz-Mezcua, B. (2019). Automatic detection of relationships between banking operations using machine learning. *Information Sciences*, *485*, 319–346. https://doi.org/10.1016/j.ins.2019.02.030

Gupta, P., Varshney, A., Khan, M. R., Ahmed, R., Shuaib, M., & Alam, S. (2023). Unbalanced Credit Card Fraud Detection Data: A Machine Learning-Oriented Comparative Study of Balancing Techniques. *Procedia Computer Science*, *218*, 2575–2584. https://doi.org/10.1016/j.procs.2023.01.231

Haddab, D. M. (2023). Detecting banking frauds with analytics and machine learning. *Business & IT*, *XIII*(1), 90–96. https://doi.org/10.14311/bit.2023.01.11

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

ismael, rawaa. (2024). Credit Fraud Recognition Based on Performance Evaluation of Deep Learning Algorithm. *Iraqi Journal for Computers and Informatics*, *50*(1), 1–5. https://doi.org/10.25195/ijci.v50i1.454

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

Joshi, A. K., Shirol, V., Jogar, S., Naik, P., & Yaligar, A. (2020). Credit Card Fraud Detection Using Machine Learning Techniques. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 436–442. https://doi.org/10.32628/cseit2063114

Kanamori, S., Abe, T., Ito, T., Emura, K., Wang, L., Yamamoto, S., Phong, L. T., Abe, K., Kim, S., Nojima, R., Ozawa, S., & Moriai, S. (2022). Privacy-Preserving Federated Learning for Detecting Fraudulent Financial Transactions in Japanese Banks. *Journal of Information Processing*, *30*(0), 789–795. https://doi.org/10.2197/ipsjjip.30.789

Kawade, D., Lalge, S., & Bharati, Dr. M. (2022). Fraud Detection in Credit Card Data Using Unsupervised Machine Learning Algorithm. *International Journal for Research in Applied Science and Engineering Technology*, *10*(5), 5249–5256. https://doi.org/10.22214/ijraset.2022.42974

Kjamilji, A., & Güney, O. B. (2023). Highly efficient secure linear algebra for private machine learning classifications over malicious clients in the post-quantum world. *Journal of King Saud University - Computer and Information Sciences*, *35*(9), 101718. https://doi.org/10.1016/j.jksuci.2023.101718

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*(9 (107)), 14–26. https://doi.org/10.15587/1729-4061.2020.212830

Kousika, N., Vishali, G., Sunandhana, S., & Vijay, M. A. (2021). Machine Learning based Fraud Analysis and Detection System. *Journal of Physics: Conference Series*, *1916*(1), 12115. https://doi.org/10.1088/1742-6596/1916/1/012115

Kumar, M. N. K., Umaswathika, A., Yaswanthkumar, K., & Madhumitha, B. (2024). A Robust Detection Fraudulent Transactions In Banking Using Machine Learning. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *15*(1), 118–122. https://doi.org/10.61841/turcomat.v15i1.14551

Kumar, P. S. G., Reddy, P. A. S., & Posonia, A. M. (2019). Credit Card Fraud Detection using Machine Learning. *International Journal of Engineering and Advanced Technology*, *9*(2), 4118–4123. https://doi.org/10.35940/ijeat.b4957.129219

Li, W., Wu, C., & Ruan, S. (2022). CUS-RF-Based Credit Card Fraud Detection with Imbalanced Data. *Journal of Risk Analysis and Crisis Response*, *12*(3). https://doi.org/10.54560/jracr.v12i3.332

Lin, D. (2023). An Empirical Analysis of Machine Learning for Fraud Detection in Diverse Financial Scenarios. *Advances in Economics, Management and Political Sciences*, *42*(1), 202–216. https://doi.org/10.54254/2754-1169/42/20232110

Lokanan, M. E., & Sharma, K. (2022). Fraud prediction using machine learning: The case of investment advisors in Canada. *Machine Learning with Applications*, *8*, 100269. https://doi.org/10.1016/j.mlwa.2022.100269

Mitra, A., Siddhant, M., & P, G. S. (2022). Credit Card Fraud Detection using Autoencoders. *YMER Digital*, *21*(06), 337–342. https://doi.org/10.37896/ymer21.06/32

Mohmad, Y. A. (2022). Credit Card Fraud Detection Using LSTM Algorithm. *Wasit Journal of Computer and Mathematics Science*, *1*(3), 26–35. https://doi.org/10.31185/wjcm.60

Mytnyk, B., Tkachyk, O., Shakhovska, N., Fedushko, S., & Syerov, Y. (2023). Application of Artificial Intelligence for Fraudulent Banking Operations Recognition. *Big Data and Cognitive Computing*, *7*(2), 93. https://doi.org/10.3390/bdcc7020093

Nageswara Rao Moparthi, S. A. (2024). Fraud Detection in Banking Data by Machine Learning Techniques. *Journal of Electrical Systems*, *20*(2), 2773–2784. https://doi.org/10.52783/jes.2056

Narsimha, B., Raghavendran, C. V, Rajyalakshmi, P., Reddy, G. K., Bhargavi, M., & Naresh, P. (2022). Cyber Defense in the Age of Artificial Intelligence and Machine Learning for Financial Fraud Detection Application. *International Journal of Electrical and Electronics Research*, *10*(2), 87–92. https://doi.org/10.37391/ijeer.100206

Nesvijevskaia, A., Ouillade, S., Guilmin, P., & Zucker, J.-D. (2021). The accuracy versus interpretability trade-off in fraud detection model. *Data & Policy*, *3*. https://doi.org/10.1017/dap.2021.3

Nwachukwu, A. S., & Boatengu, K. E. (2022). How banks are leveraging machine learning: perspective from African banks. *Business & IT*, *XII*(1), 219–225. https://doi.org/10.14311/bit.2022.01.26

Ojugo, A. A., Akazue, M. I., Ejeh, P. O., Ashioba, N. C., Odiakaose, C. C., Ako, R. E., & Emordi, F. U. (2023). Forging a User-Trust Memetic Modular Neural Network Card Fraud

Detection Ensemble: A Pilot Study. *Journal of Computing Theories and Applications*, *1*(2), 1–11. https://doi.org/10.33633/jcta.v1i2.9259

Ojulari, H. O., Oke, A. O., & Arulogun, O. T. (2024). Detecting Fraud in Automated Teller Machine Transactions in the Nigerian Bank System Using Unsupervised Deep Learning. *Advances in Multidisciplinary & Scientific Research Journal Publications*, *15*(2), 1–14. https://doi.org/10.22624/aims/cisdi/v15n2p1

Ore-Areche, F., Muñoz-Alejo, K. N., & Puma-Condori, C. (2022). Analysis and Detection of Fraud in Credit Card Using SILOF. *INTERNATIONAL RESEARCH JOURNAL OF ENGINEERING & APPLIED SCIENCES*, *10*(3), 34–41. https://doi.org/10.55083/irjeas.2022.v10i03006

Paladini, T., Monti, F., Polino, M., Carminati, M., & Zanero, S. (2023). Fraud Detection under Siege: Practical Poisoning Attacks and Defense Strategies. *ACM Transactions on Privacy and Security*, *26*(4), 1–35. https://doi.org/10.1145/3613244

Parmar, J., C. Patel, A., & Savsani, M. (2020). Credit Card Fraud Detection Framework - A Machine Learning Perspective. *International Journal of Scientific Research in Science and Technology*, 431–435. https://doi.org/10.32628/ijsrst207671

Patil, S., Nemade, V., & Soni, P. K. (2018). Predictive Modelling For Credit Card Fraud Detection Using Data Analytics. *Procedia Computer Science*, *132*, 385–395. https://doi.org/10.1016/j.procs.2018.05.199

Patil, T., & Khadare, K. (2023). Credit Card Fraud Detection. *International Journal of Scientific Research in Science and Technology*, 938–942. https://doi.org/10.32628/ijsrst523102150

Ponaganti, M. (2019). CREDIT CARD FRAUD PREDICTION FOR BANKS USING ABNORMALITY AND REGRESSION ALGORITHM WITH WEBAPP. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *10*(2), 1180–1186. https://doi.org/10.61841/turcomat.v10i2.14506

Prof. Antara Bhattacharya, Kartik Bhandari, Aranya Kawale, Maithili Kontamwar, Aditi Chowbey, & Mohd. Shahwaz Mansuri. (2023). Bank Loan Fraud Detection with Integrated KYC Verification System. *International Journal of Advanced Research in Science, Communication and Technology*, 51–60. https://doi.org/10.48175/ijarsct-13609

Rahangdale, S., Gedam, S., Pusam, D., & Harne, P. (2022). Machine Learning for Credit Card Fraud Detection System. *International Journal of Advanced Research in Science, Communication and Technology*, 418–422. https://doi.org/10.48175/ijarsct-5365

Rahmatullah, Moh. B. S., Hanani, A. L. S., Naim, A. M., Sari, Z., & Azhar, Y. (2022). Detection of Credit Card Fraud with Machine Learning Methods and Resampling Techniques. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *6*(6), 923–929. https://doi.org/10.29207/resti.v6i6.4213

Rode, Y., Jadhav, M., Jain, P., Kanase, O., & Phalake, V. S. (2022). Study on Fraud Transaction Detection System. *International Journal of Advanced Research in Science, Communication and Technology*, 209–212. https://doi.org/10.48175/ijarsct-3244

Sahu*, S., agarawal, D. shikha, & Baraskar, Dr. R. (2019). The Effect of Best First Search Optimization on Credit Card Fraudulent Transaction Detection. *International Journal of Innovative Technology and Exploring Engineering*, *8*(12), 1939–1946. https://doi.org/10.35940/ijitee.l2894.1081219

Sasikala, G., Laavanya, M., Sathyasri, B., Supraja, C., Mahalakshmi, V., Mole, S. S. S., Mulerikkal, J., Chidambaranathan, S., Arvind, C., Srihari, K., & Dejene, M. (2022). An Innovative Sensing Machine Learning Technique to Detect Credit Card Frauds in Wireless

Communications. *Wireless Communications and Mobile Computing*, *2022*, 1–12. https://doi.org/10.1155/2022/2439205

Shah, A., & Mehta, A. (2021). Comparative Study of Machine Learning Based Classification Techniques for Credit Card Fraud Detection. *2021 International Conference on Data Analytics for Business and Industry (ICDABI)*, 53–59. https://doi.org/10.1109/icdabi53623.2021.9655848

Shah, D., & Sharma, L. K. (2023). Credit Card Fraud Detection using Decision Tree and Random Forest. *ITM Web of Conferences*, *53*, 2012. https://doi.org/10.1051/itmconf/20235302012

Shmatko, O., Fedorchenko, V., & Prochukhan, D. (2021). DETECTING CREDIT CARD FRAUD USING MACHINE LEARNING ALGORITHMS. *InterConf*, 393–403. https://doi.org/10.51582/interconf.19-20.08.2021.037

Smiles*, J. A., & Kumar, Dr. A. S. (2019). Synthetic Minority Oversampling and Smote Regularised Deep Autoencoders Neural Network Techniques for Fraud Prediction in Financial Payment Services. *International Journal of Innovative Technology and Exploring Engineering*, *8*(12), 2915–3908. https://doi.org/10.35940/ijitee.l3419.1081219

Sudhakar, M., & Kaliyamurthie, K. P. (2023). A Novel Machine learning Algorithms used to Detect Credit Card Fraud Transactions. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(2), 163–168. https://doi.org/10.17762/ijritcc.v11i2.6141

Sultana, S., Rahman, S., & Afroj, M. (2023). An efficient fraud detection mechanism based on machine learning and blockchain technology. *2023 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, 162–168. https://doi.org/10.1109/3ict60104.2023.10391306

Suri*, T., Singh, S., Singh, T., Rajappan, A. K., & Florence, Dr. S. M. (2020). An Effective Method to Understand Bank Customer Retention System. *International Journal of Recent Technology and Engineering (IJRTE)*, *8*(6), 4279–4283. https://doi.org/10.35940/ijrte.f8947.038620

T, S., Nath, B. N., Manjunath, N, G., & Kumar, H. V. N. (2022). Detection of Credit Card Fraud Transactions using Machine Learning based Algorithm. *International Journal of Advanced Research in Science, Communication and Technology*, 666–671. https://doi.org/10.48175/ijarsct-5742

Thilakaratne, M., Falkner, K., & Atapattu, T. (2019). A systematic review on literature-based discovery workflow. *PeerJ Computer Science*, *5*, 1–40. https://doi.org/10.7717/peerj-cs.235

Togbe, M. U., Chabchoub, Y., Boly, A., Barry, M., Chiky, R., & Bahri, M. (2021). Anomalies Detection Using Isolation in Concept-Drifting Data Streams †. *Computers*, *10*(1), 13. https://doi.org/10.3390/computers10010013

Tran, L., Tran, T., Tran, L., & Mai, A. (2019). Solve fraud detection problem by using graph based learning methods. *ArXiv*. https://doi.org/10.48550/arxiv.1908.11708

Usman, A. U., Abdullahi, S. B., Liping, Y., Alghofaily, B., Almasoud, A. S., & Rehman, A. (2024). Financial Fraud Detection Using Value-at-Risk with Machine Learning in Skewed Data. *IEEE Access*, *PP*(99), 1. https://doi.org/10.1109/access.2024.3393154

Vanini, P., Rossi, S., Zvizdic, E., & Domenig, T. (2023). Online payment fraud: from anomaly detection to risk management. *Financial Innovation*, *9*(1), 66. https://doi.org/10.1186/s40854-023-00470-w

Venkata Suryanarayana, S., N. Balaji, G., & Venkateswara Rao, G. (2018). Machine Learning Approaches for Credit Card Fraud Detection. *International Journal of Engineering & Technology*, *7*(2), 917. https://doi.org/10.14419/ijet.v7i2.9356

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

Waykar, M. (2023). Fraud Detection using IBMs Differential Privacy Library. *International Journal for Research in Applied Science and Engineering Technology*, *11*(10), 749–754. https://doi.org/10.22214/ijraset.2023.56095

Wei, P. (2023). SVM Model Against Telecom Card Fraud Using GA Optimised Ten-Fold Cross-Testing. *Highlights in Science, Engineering and Technology*, *70*, 123–132. https://doi.org/10.54097/hset.v70i.12169

Xiang, S., Zhu, M., Cheng, D., Li, E., Zhao, R., Ouyang, Y., Chen, L., & Zheng, Y. (2023). Semi-supervised Credit Card Fraud Detection via Attribute-Driven Graph Representation. *Proceedings of the AAAI Conference on Artificial Intelligence*, *37*(12), 14557–14565. https://doi.org/10.1609/aaai.v37i12.26702

Zareapoor, M., & Shamsolmoali, P. (2015). Application of Credit Card Fraud Detection: Based on Bagging Ensemble Classifier. *Procedia Computer Science*, *48*, 679–685. https://doi.org/10.1016/j.procs.2015.04.201

Zhang, J. (2023). Credit Card Fraud Detection Using Predictive Model. *BCP Business & Management*, *38*, 2820–2826. https://doi.org/10.54691/bcpbm.v38i.4196