Application of AI techniques for the detection of banking fraud: an investigation*

Fèmi José DJAMBOUTOU[1,*,†] and Pélagie HOUNGUE[2,†]

[1] *Ecole Doctorale des Sciences de l'Ingénieur, Université d'Abomey-Calavi, Abomey-Calavi, Benin*
[2] *Institut de Mathématiques et de Sciences Physiques (IMSP), Dangbo, Benin*

Abstract

Cyber fraud is a major concern for banking industry players. Banks are subject to cyber-attacks in all their forms (credit card fraud, money laundering, identity fraud, check fraud, internal fraud, etc.). This situation causes the attrition of hard-won customers. Financial losses amount to around $1 trillion per year worldwide. The increase in volume and value of attacks against banking institutions justifies the need to use Artificial Intelligence (AI) techniques. This article reviews and summarizes the advances in the application of AI to banking fraud detection. A total of 19 scientific articles published between 2008 and 2025 and relevant to the review served as a source of information. Our work highlighted the appropriate AI techniques to address each type of banking fraud. The GBoost -ADSYN (99.94%), HFS-LGBM (98.72%), XGBOOST graph (95%) and XGBoost Optimized (99.68%) models show the best performance in combating bank credit card fraud, identity fraud, money laundering problem and internal fraud in banking institutions respectively. The study also focused on identifying the limitations of using AI in bank fraud detection through a SWOT analysis. Recommendations and directions for future research were provided accordingly.

Keywords

Bank fraud, artificial intelligence, deep learning, machine learning

1. Introduction

The digital age is accompanied by an increase in crimes and attacks against banking institutions. According to McKinsey, losses due to banking fraud worldwide could approach $1 trillion by 2025 [1]. Disarray spares no nation in modern civilizations. Banking globalization has a bitter aftertaste, marked by financial crimes of all kinds [2]. The worst-case scenario is to be feared in underdeveloped countries where banking systems struggle to cope with criminals and their fraud techniques. The consequences are perceptible on the performance of banking activities and on the health of economies worldwide. In many ways, this is a new problem that escapes the attention of banking sector players and the scientific community. Since 1970, a variety of traditional knowledge-based approaches such as Personal Identification Number (PIRN), passwords, and other similar methods have been made available [3]. Yet, bank fraud cases continue to increase in volume and value.

Recently, AI approaches have emerged to counter the evolving landscape of financial crime. A study by McKinsey projects a significant profit of $340 billion for the banking sector. Several research studies are devoted to this new trend and the results are convincing. However, there is no recent synthesis of the advances in the application of AI to banking fraud. While it is necessary for banking sector stakeholders, IT security experts and scientists to have a recent synthesis of this previous work in order to promote a prompt response to threats. The objective of this article is to analyze the growing effectiveness of the use of AI in the fight against banking fraud by answering the following research questions:

* *CITA 2026 - Land, Smart Cities, and Sustainable Development, 25-26 June 2026, Cotonou, Benin*
[1]* Corresponding author.
† These authors contributed equally.
djamboutoujose@gmail.com (F. J. DJAMBOUTOU); pelagie.houngue@imsp-uac.org (P. HOUNGUE)
0009-0003-4315-3576 (F. J. DJAMBOUTOU); 0000-0001-8138-2079 (P. HOUNGUE)

- What AI approaches are commonly deployed to detect and prevent banking fraud?
- What types of banking fraud are targeted by AI-based methods?
- Which AI techniques seem best suited to tackle each type of banking fraud?
- How does the performance (precision, recall, F1-score) of AI models vary across application techniques and contexts?
- What are the advantages and limitations of AI techniques applied to banking fraud detection according to existing literature?

These are all questions whose answers would allow for a synthesis of the existing literature. It should be noted that some authors have conducted systematic review studies in the field. However, existing reviews are either outdated and do not take into account recent discoveries, or they are restrictive and omit certain methodological aspects of the application of AI to banking fraud. This document attempts to fill these gaps through the four sections: (I) research methodology; (II) types of banking fraud and application of AI; (III) limitations of the study; (IV) discussion.

2. Research methodology

The documents used as data sources for writing this systematic review are mainly scientific articles published between 2008 and 2025. The Scopus, Google Scholar and Web of Science (WOS) databases were mainly used as sources of information. The following search string was used to collect documents from the different publication databases: (Bank fraud AND artificial intelligence) or (Bank fraud AND Deep learning) or (Bank fraud AND machine learning). A total of 365 scientific articles were obtained from the various targeted sources. The analysis of the documents was carried out according to the PRISMA criteria (Preferred Reporting IEMS for Systematic Reviews and Meta Analysis). After applying the inclusion and exclusion criteria, 19 documents were found to be eligible for the study. A systems approach was adopted for information extraction and analysis. Figure 1 below illustrates documents analysis process using the PRISMA method.

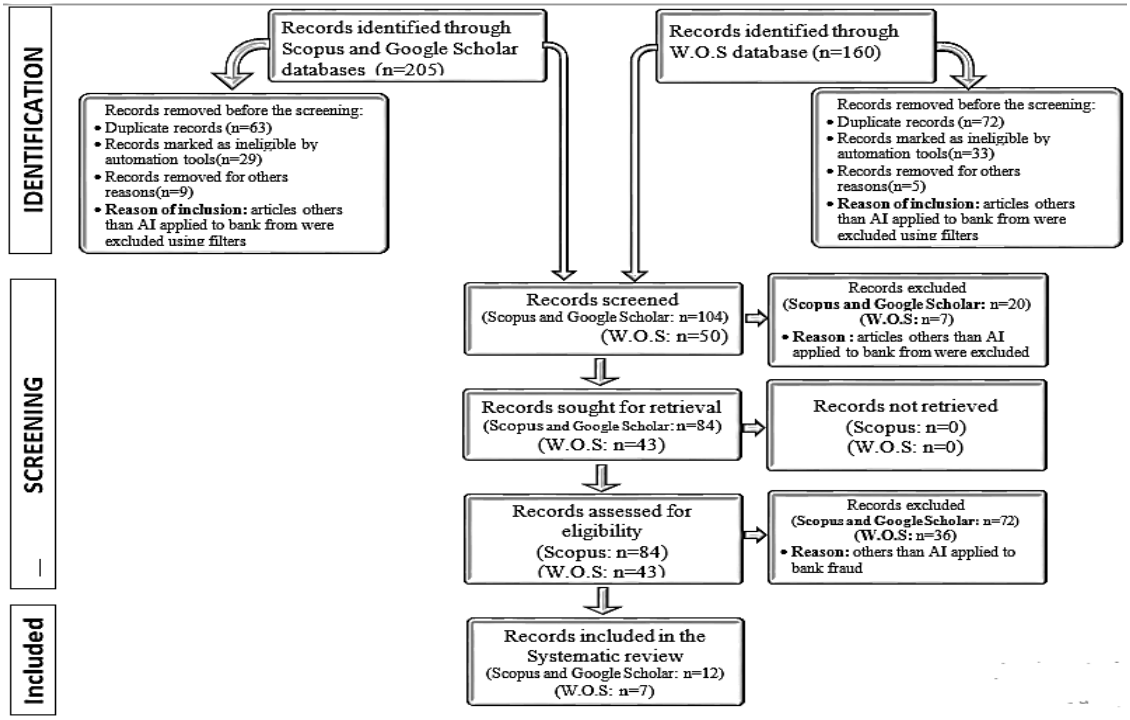

Figure 1: Documents analysis process using the PRISMA method

3. Results

The purpose of this section is to present the results of the investigation.

3.1. Types of Bank Fraud and AI Approaches

Over the years, criminals have developed a multitude of banking fraud techniques. The evolution of fraud strategies is as spectacular as it is enigmatic. Techniques are refined, modernized, and adapted to specific fraud conditions. Fraudsters are one step ahead of their detractors. An exploration of the literature shows that banking fraud techniques can be divided into seven broad categories: credit card fraud, check fraud, identity fraud, internal fraud, phishing fraud, money laundering, cryptocurrency fraud, and online platform fraud. The 19 scientific articles deemed eligible for study were categorized by banking fraud to facilitate systematic analysis.
Bank credit card fraud ranks first with 10 articles. Internal fraud follows with 4 articles. Identity fraud and money laundering come last with 3 articles and 2 articles respectively. Figure 2 shows the trends.

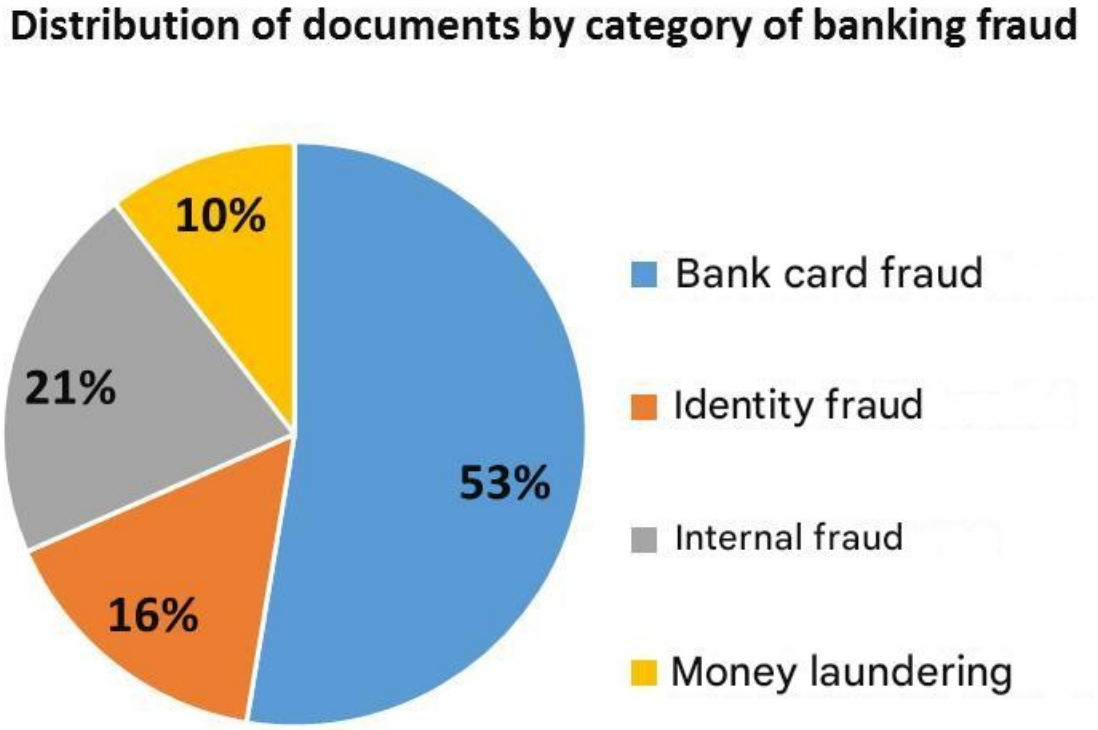

Figure 2: Distribution of eligible documents by category of banking fraud

The figure above gives a clear idea of the scope of research in this field. The graph shows that bank card fraud occupies a significant portion of this universe with 53% of eligible documents. This explains the growing interest of researchers in solving this problem. Productions in the fields of internal fraud and identity fraud occupy second and third place respectively with 21% and 16% of eligible documents. This means that these two fraud techniques appear to be of lesser importance compared to the first. As for the other categories of bank fraud, they require specific skills to implement. They are unpopular and claim fewer victims. This state of affairs justifies the fact that very few documents are devoted to them.

This, in brief, is the breakdown of the scientific articles eligible for the study. In the remainder of the document, we will conduct a systematic, problem-oriented approach, where each fraud category constitutes a unit of analysis. We begin the presentation with bank credit card fraud.

3.1.1. Bank credit card fraud and unauthorized payments

The graph in the previous section shows that bank credit card fraud dominates the anti-bank fraud literature. According to a study by the French Ministry of Internal Security, this form of fraud represents 14.5% of payment scams and frauds. The rapid rise of the phenomenon has its origins in

the hidden side of the Internet, also called the darknet. There, there are a plethora of fraudsters offering to sell counterfeit or stolen bank cards. It is a vast market with a turnover exceeding 630 billion dollars per year [4]. Bank card fraud involves the unauthorized use of credit card information to carry out transactions. The research mission is to quickly detect suspicious transactions before they cause significant financial losses. The objective of this section is to present the findings of techniques and methods of the scientific community to deal with the problem of bank credit card fraud. To provide a better reading experience, we recommend organizing this part of our document into subsections. To do this, a close analysis of the documents allowed us to classify the articles into three categories: scientific articles proposing new models, scientific articles dedicated to improving existing techniques, and scientific survey articles intended to identify the best algorithms. Figure 3 illustrates this classification.

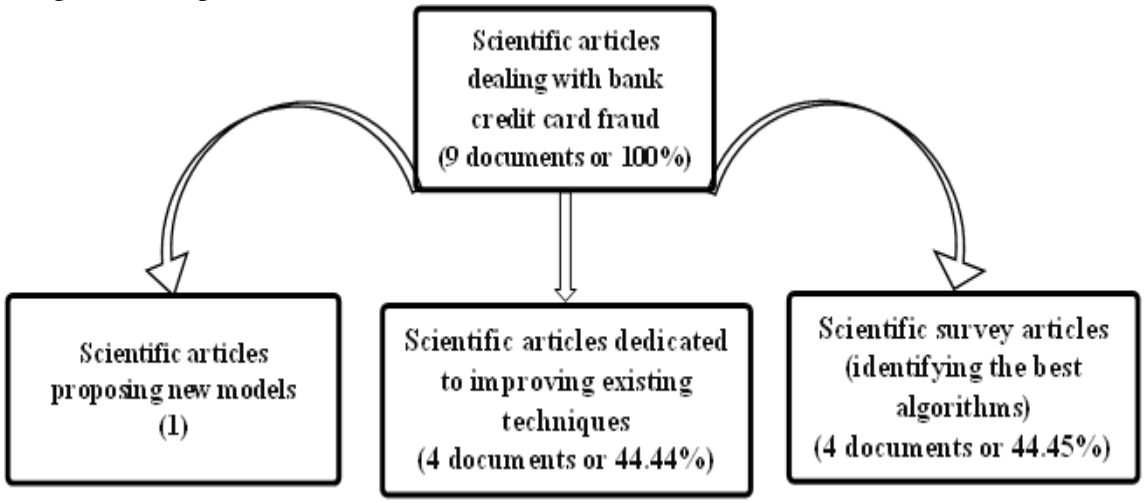

Figure 3: Distribution of scientific articles dealing with bank credit card fraud

The rest of the section is organized along the three axes identified above.

- Creation of new models

In a delicate research field like AI, creating a new technique is considered a bold undertaking. Especially when it comes to AI applied to bank credit card fraud detection, the risks of abandonment are high due to the many obstacles related to the banking sector. Nevertheless, some researchers venture into it and obtain convincing results. This was the case of HaiChao Du et al. in 2024. The idea was to develop a model based on Autoencoder and XGBoost combined with SMOTE and CGAN to improve fraud detection. A 2% improvement in accuracy was observed compared to other methods. Their work also achieved a 30% increase in MCC compared to KNN [5]. However, the comparison was limited to some classical algorithms. This could influence the generalization of the result. Another trend in this sector is the improvement of existing models.

- Optimization of existing techniques and methods

Credit card-based crime is the most dynamic form of banking fraud. Fraudsters are constantly improving their methods to evade the security measures deployed within banking institutions. It is therefore essential for researchers and cybersecurity professionals to regularly update existing solutions. At this level, the work consists of making significant improvements to previous findings. Those involved in this exercise face the same challenges as the previous category, with the only difference being that the latter is less perilous. The ADASYN and Recursive models Feature Elimination models received this type of update, sometime in 2024. This was part of a collaborative effort led by Emmanuel Ileberi and Yanxia Sun. The researchers aimed to improve model performance by combining ADASYN, which is an oversampling technique, with recursive feature

elimination and cross-validation. The experiment showed significant improvement, including Extreme Gradient Boosting with an MCC of 99.94%. However, the experiment requires further validation on more diverse datasets [6].

Furthermore, hyperparameters are parameters that are defined before the training process of a model. Unlike other parameters that are learned automatically during training, hyperparameters are set manually and directly influence the learning behavior. Although hyperparameters vary across models, it is important to ensure their optimization to ensure better results in bank fraud detection. This was the case of Dijana Jovanovic et al. (2022) who contributed to the optimization of ML models using an improved Firefly algorithm. The proposed model significantly improves classification [7]. However, the results from the experiment vary depending on the dataset used. G. Sasikala et al. (2022) conducted a similar study by optimizing SVM hyperparameters. An improvement in fraud detection was observed, particularly through the use of linear, Gaussian, and polynomial kernels [8]. As a limitation of this study, the method is sensitive to the choice of SVM parameters and requires precise tuning to avoid overfitting. Similarly, Hemant Palivela et al. (2024) attempted to optimize a deep model learning for fraud detection. The results are convincing with an accuracy reaching 99.59% thanks to advanced preprocessing and feature engineering techniques [9]. The experiment needs validation on a more diverse dataset. The last category in this section concerns scientific survey articles.

- Scientific articles for surveys

The idea behind this type of research is to consider a number of algorithms or models to determine the best one under the conditions of the experiment. The evaluation methodology is heavily based on the comparison of certain parameters deemed. For example, a study by Abdul Salam et al. relies on accuracy to compare the performance of Random Forest (RF), Logistic Regression, K- Nearest Neighbors (KNN), Decision Tree (DT) and Gaussian Naive Bayes (NB). The algorithms achieved accuracies of 99.99%; 94.61%; 99.96%; 99.98% and 91.47% respectively in bank card fraud detection [10]. A comparison of the results reveals that RF outperforms with high performance parameters (accuracy, recall, precision and f-score) better than NB; RF; DT and KNN. Random Forest then exhibits high performance for bank credit card fraud detection with minimal loss values. In the same perspective, Pratyush Sharma al. (2021) compared different machine learning methods for credit card fraud detection. The Artificial Neural Network (ANN) achieved the best F1 score of 0.91. The dataset used underwent dimensional reduction via PCA, limiting the analysis of specific attributes [11]. Also, Emmanuel Ileberi (2021) performed the same exercise by comparing several ML methods using SMOTE and AdaBoost to improve fraud detection. AdaBoost significantly improved classification. The limitations of the study are problems related to over-fitting of models [12].

Muhammad Adil et al. agree with their article published in 2024. The work was intended to be exhaustive by first evaluating existing models and then proposing an optimized neural network. The proposed model outperformed other algorithms in terms of accuracy [13]. The study is limited by the risks of false positives and false negatives.

In short, the scientific community is aware of the urgent need to find solutions to the problem of bank credit card fraud. It is with this in mind that AI is being used. In the literature, we discovered three categories of documents dealing with bank credit card fraud. But it is important to remember that the categorization of scientific articles was undertaken for practical reasons. It has no connection with the actual performance of the algorithms. Speaking of performance, it would be interesting to determine the algorithm or model that seems most suited to solving the problem of bank credit card fraud. Also, for practical reasons, we opted for the "accuracy" parameter as the criterion for comparing the algorithms or models in this section. The graph in Figure 4 shows an overview of the performance of AI technologies dedicated to solving the problem of bank credit card fraud.

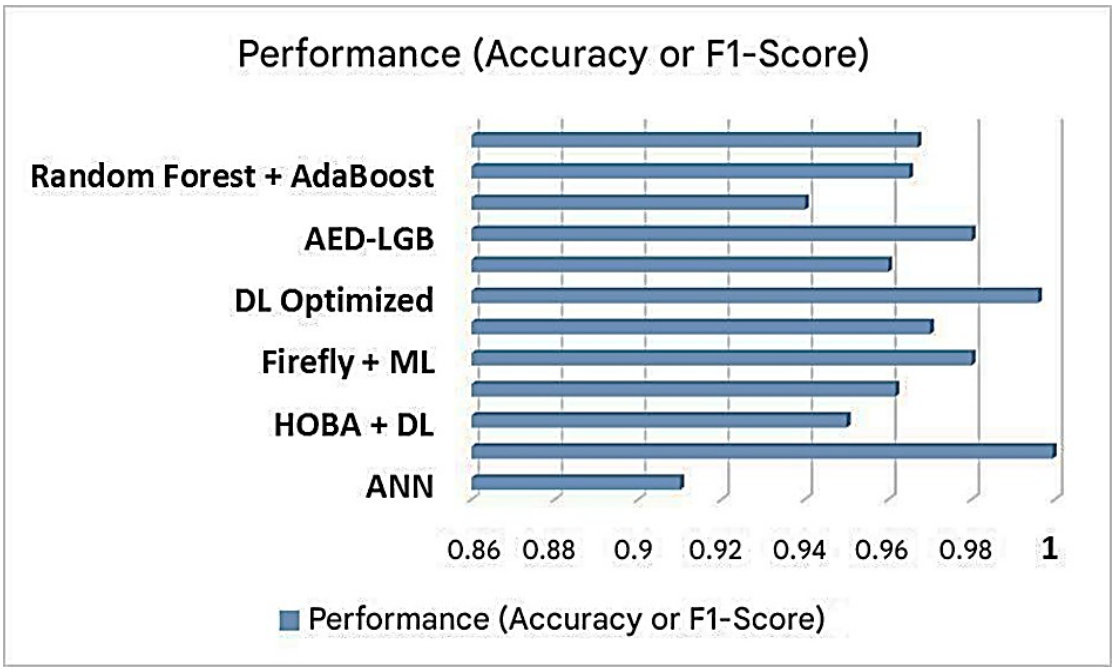

Figure 4: Overview, in terms of accuracy, of the performance of AI technologies dedicated to solving the problem of bank credit card fraud

GBoost -ADSYN model has the best performance of 99.94% in detecting bank credit card fraud.

3.1.2. Identity fraud or identity theft

Identity fraud is the misuse of personal information by a fraudster to exploit one or more existing accounts. Identity theft involves a fraudster stealing someone else's personal information to open and use new accounts. The difference is subtle, but the two categories of fraud should not be confused. However, these types of fraud are likely to allow criminals to open and use lines of credit in the name and on behalf of their victims. This can have serious consequences, particularly for the victim. Identity theft attacks have become a major concern for online banking providers. AI is being used to combat this form of banking fraud. With this in mind, Argolo Bonfim et al. (2021) proposed an improvement of the Biotouch framework for continuous authentication based on dynamic touch biometrics in mobile banking applications. The study methodology was based on the use of a multimodal framework with supervised learning. Data collection was done through the Android application. Biotouch. The results of the study show an accuracy varying between 82.53% and 96%, an equal error rate (EER) between 1.88% and 9.85% and the F1 score is between 90.68% and 97.05%. However, the observed results must be taken with a pinch of salt because the performance of the application varies according to the users. To this must be added the need to access more data for certain scenarios while the test is carried out on a limited sample of 51 users. This could bias the results [14].

Pursuing the objective of solving the identity theft problem during banking transactions, G. Logeswari et al. (2022) developed a machine learning-based intrusion detection system (IDS) for software-defined networks (SDN). They used the HFS-LGBM algorithm that combines correlation-based feature selection (CFS) and recursive feature elimination (RF-RFE). The results show a precision of 98.72%; a recall of 97.92% and an F-measure of 98.23%. The experiment reveals a better performance of their technique compared to other tested algorithms such as SVM and XGBoost [15]. One of the limitations of the study is related to the fact that the technique is only tested on an NSL-KDD dataset. The other limitation is the high computational complexity for wide area networks. The scenarios were simulated only in Mininet and this does not provide reassurance in terms of the reliability of the results.

Ali Raza and his collaborators performed the same exercise in a scientific article published in 2021. They proposed a hybrid approach to detecting faked images. The approach is based on the hybridization of VGG16 and convolutional neural networks. The technique was evaluated on a dataset of real faces and faces faked with Photoshop. The results show a precision of 95% and an accuracy of 94%. We note a better performance of this hybrid method, compared to other transfer learning methods such as Xception, NAS net, MobileNet and VGG16. As a lack of experience, the test was limited to a specific dataset (real faces and fake faces). To this must be added the risk of overfitting and the strong dependence of the results on the quality of the training data used [16].

In summary, the authors have made significant contributions to solving identity theft problems. The aforementioned research findings could prevent fraudsters from opening and exploiting credit lines in the name and on behalf of their victims. However, a question arises: which of the methods explored can be considered the most suitable for detecting this category of fraud? This is a difficult question to answer, given the multitude of parameters that could come into play. For practical reasons, we consider for this exercise, "accuracy" as a variable for comparing the different methods in order to answer the question. The graph in Figure 5 presents a comparative overview of the performances, in terms of accuracy, of the technologies proposed by the scientific community in the fight against identity fraud.

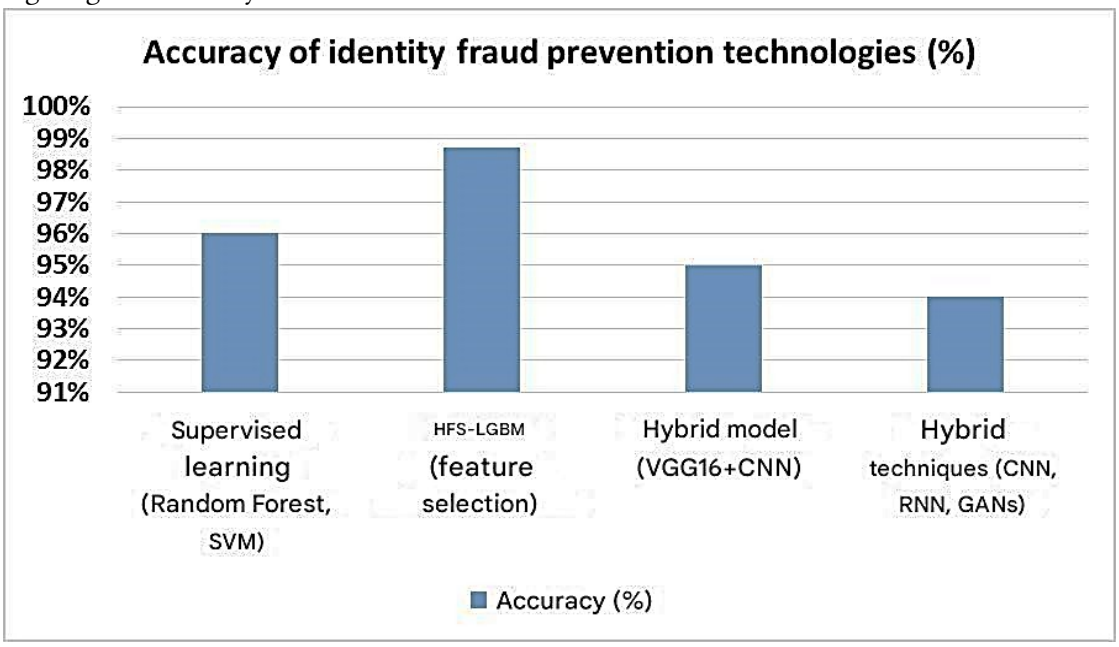

Figure 5: Comparative study of the performance, in terms of accuracy, of technologies for combating identity fraud

The HFS-LGBM technique, based on feature selection, stands out as the best solution for this category of fraud with an accuracy of 98.72%. Supervised learning follows with an accuracy of 96%. The other models and hybrid techniques occupy the last places with 95% and 94% accuracy.

3.1.3. Money laundering

Money laundering is a process by which criminals conceal the illicit origin of funds through complex transactions. The United Nations (UN) estimates that 2 to 5% of global GDP, or approximately $2 trillion, is laundered globally each year [17]. This fraud is particularly difficult to detect due to the diversity of transaction behaviors involved. The complexity is such that a single artificial intelligence technique cannot address the problem. In the majority of cases, the use of hybrid technologies is necessary to achieve good detection performance. Only a small fraction of research deals with the subject, i.e. 10% of eligible documents. During 2022, a hybrid active learning technique was developed to predict money laundering cases with reduced costs. The technique is

known as Amaretta. It combines supervised and unsupervised learning algorithms. The algorithm was tested on a synthetic dataset of financial transactions. The performance of the algorithm was compared with AI2 and other conventional fraud detection methods. The technique is found to be better compared to traditional and AI2 methods with an increase in detection rate of 50% and a reduction in costs of 20% [18]. However, the use of synthetic dataset limits the generalization to real cases.

Another interesting study was conducted in 2024 by Md. Rezaul et al. Their approach was based on semi-supervised graph learning and aimed to detect money laundering activities. Graph learning algorithms such as SkipGCN, FastGCN, and EvolveGCN were used. The algorithm was tested on synthetic and real-world datasets such as Amlin , Elliptic , IBM AML, and SynthAML . Then, the results were compared with traditional machine learning techniques. EvolveGCN is found to perform better end-to-end with a better ability to detect suspicious transactions [19] . The difficulty in accessing real-world data due to privacy restrictions limits the reliability of the results of this study.

It would be interesting to compare the different technologies discussed in this section to determine the best one. To do this, accuracy was chosen as the comparison tool. The graph in Figure 6 provides a clear overview of the situation.

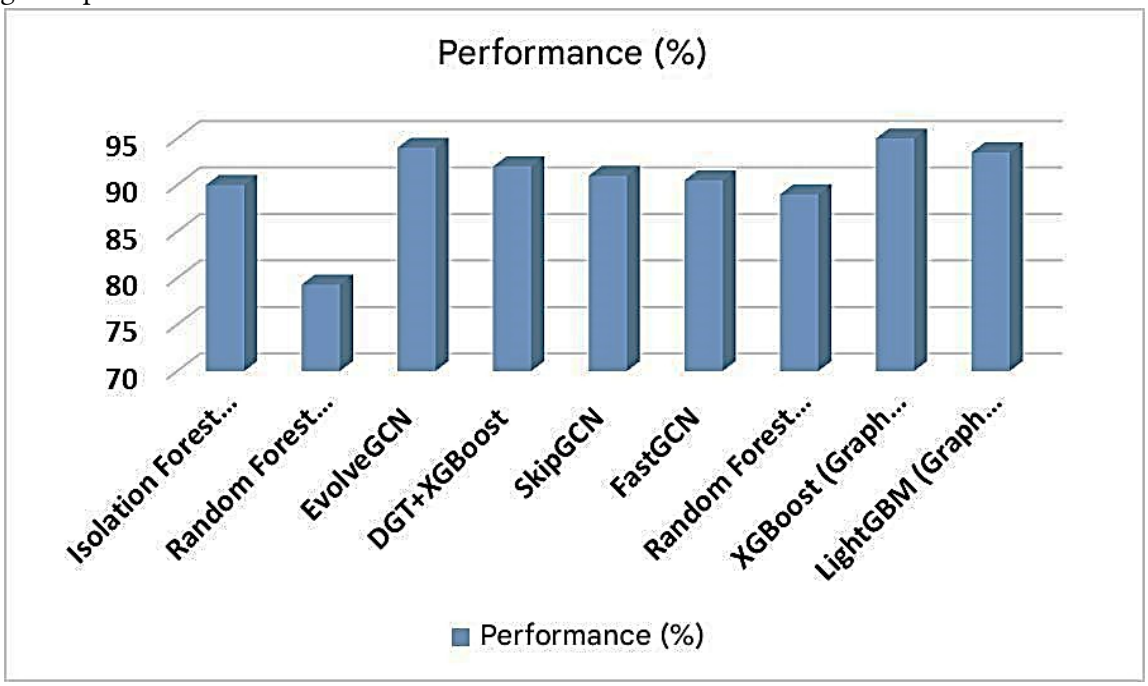

Figure 6: Comparative study of the performance, in terms of accuracy, of anti-money laundering technologies

From the graph, we can deduce that XGBoost dominates the other techniques with an accuracy of 95%. This algorithm seems better suited for solving the money laundering problem. LightGBM ranks second with an accuracy of 93.5%. This latter technique could be used as a substitute for XGBoost, since the performance gap between the two technologies is not large enough. The other algorithms have performances between 89% and 92%.

3.1.4. Internal fraud (collision)

Internal fraud originates from employees or banking partners. They exploit loopholes in the system to commit fraudulent acts. Detecting this fraud requires an approach capable of analyzing internal transactions and identifying collusive behavior. Graph-based models analyze the relationships between different transaction entities. These models have proven effective in identifying collusive behavior in complex transaction networks. As proof, the Random Forest model with SMOTE

performed well in an experiment conducted by Serhan. Hamal and Ozlem Senvar in 2021. The objective of their research was to evaluate the effectiveness of machine learning classifiers in detecting financial accounting fraud [19]. Classical classifiers like SVM, Naive Byes, neural networks, KNN, Random Forest, logistic regression and Bagging were tested in the. The Random Forest with SMOTE presents the best performances for the experiment. It is important to emphasize that the results depend heavily on the data used. The other challenge of this research is the class imbalance which could bias the results. In the same perspective, Muath Asmar et al. (2024) set out to study the integration of machine learning algorithms in cyber security measures of digital banks by analyzing the advantages and disadvantages. The study involved the analysis of relevant machine learning algorithms (SVM, RNN, HMM, LOF). As a result, machine learning enabled faster and more efficient detection of cyber-attacks. But challenges related to interpretability and adversarial attacks remain [20].

A study by Dimitrios Kotios et al. (2022) used a cash flow forecasting model based on recurrent neural networks (deepAR RNN). The authors developed a hybrid transaction categorization and cash flow forecasting model to improve the financial management of SMEs in the banking sector. The study reveals that the hybrid CatBoost+DeepAR model improves the accuracy of transaction classification and cash flow forecasting. The challenges related to this experiment are the lack of open datasets, a limitation related to the reproducibility of the experiment, the sensitivity of cash flow forecasts to market fluctuations and unpredictable economic behavior [21].

In 2022, Surjeet Dalal et al. experimented with the optimized nature-inspired XGBoost model on a synthetic dataset of financial transactions (Banksim). They achieved an accuracy of 99.68%, outperforming other models such as Bayesian network, random forests, and logistic regression. The performance was evaluated with a 10-fold cross-validation approach and comparison with other machine learning algorithms. The model significantly reduces the error rate in predicting financial fraud. The major limitation of this technology is that the implementation of the model in banks varies according to internal and regulatory constraints. Added to this is the fact that the models require continuous updating to adapt to new forms of fraud [4].

Figure 7 presents a comparative study of the performance, in terms of accuracy, of the internal fraud prevention technologies studied in this section.

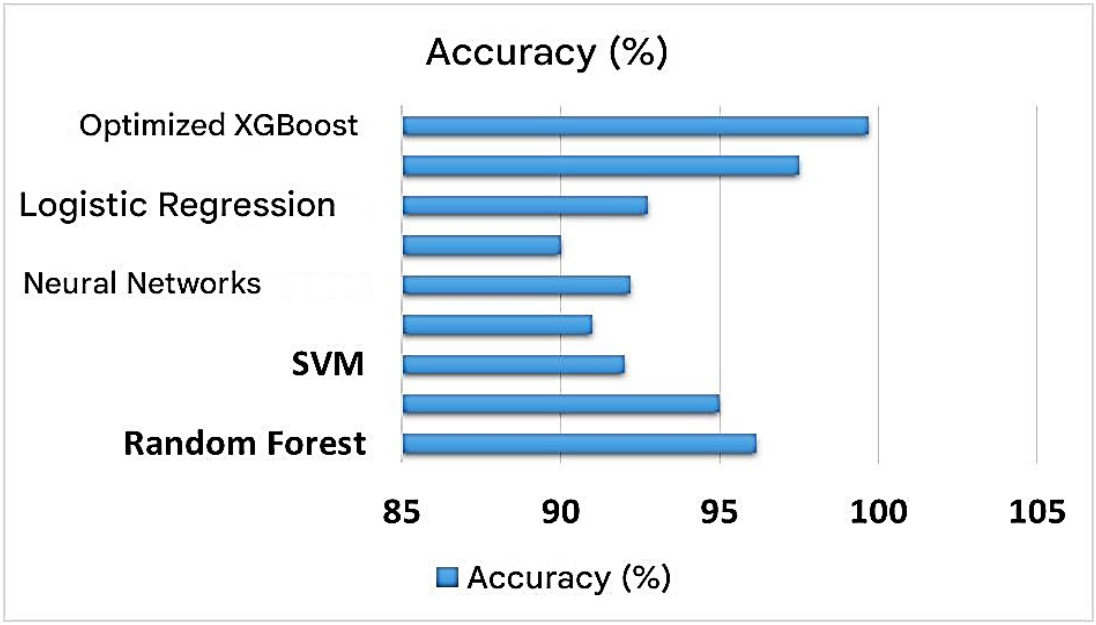

Figure 7: Comparative study of the performance, in terms of precision, of internal fraud prevention technologies

The graph allows a visual comparative approach to the performance of AI technologies applied to the detection of internal fraud within banks. The data used as a basis for the creation of the

graph come from the 4 scientific articles presented in this section. The parameter "accuracy" is chosen as a comparison variable given its importance in evaluating the performance of machine learning algorithms. From the observation of the graph in Figure 6, the optimized XGBoost technique ranks first with an accuracy of 99.68%. The technique resulting from a hybridization between CattBoost and DeepAR follows with a detection capacity of 97.5%. Random Forest, bagging, logistic regression, neural networks, SVM, Naïve Bayes and KNN do not disappoint with respective detection capacities of 96.15%; 95%; 92.73%; 92.18%; 92%; 91% and 90%. So, optimized XGBoost proposed by Surjeet Dalal et al., seems to are suitable for solving the problem of internal fraud.

These are the main findings of our research, presented in a few pages. However, it would be interesting to supplement this work by identifying the strengths, weaknesses, opportunities, and threats associated with applying AI technologies to banking fraud.

3.2. SWOT analysis of the application of AI to bank fraud

All the scientific articles consulted as part of this systematic review address the limitations that the experiments have encountered. These limitations are of various origins. Some are caused by internal factors while others are linked to factors external to banks. We speak of weaknesses or threats to the application of AI to banking fraud. On the other hand, the use of AI in the detection of banking fraud represents a real obstacle for the sector. Financial losses are considerably reduced and customers are becoming more and more confident. We speak of strengths or opportunities of the application of AI to banking fraud. A SWOT analysis made it possible to clearly identify the strengths, weaknesses, opportunities and threats of the application of AI to banking fraud. Table 1 presents the results of the analysis.

Table 1
SWOT analysis of the application of AI to banking fraud

Forces	Weaknesses
Fast, real-time fraud detection	Risks of false positives/false alerts
Continuous improvement through machine learning	Need large amounts of data to be efficient
Reduction of financial losses for banks and customers	High development and maintenance costs
Ability to analyze massive volumes of transactions	Difficulty interpreting decisions made by AI models (they behave like black boxes)
Opportunities	**Threats**
Strengthening customer confidence in banking security	Rapid evolution of fraud techniques requiring constant adaptation
Automation of controls to reduce human workload	Ethical and regulatory risks related to the use of personal data
Collaboration between banks and researchers to improve detection	Attacks on AI models aimed at deceiving them

The SWOT analysis served as a basis for identifying future work.

4. Future work

From the SWOT analysis conducted in the previous section, it is deduced that future research should focus on three major challenges: the use of transfer learning, the development of hybrid models and the security of banking data. It should also be noted that our research has limitations.

5. Limitations of the systematic review

The study was conducted based on information sources such as Scopus, Google Scholar and WOS. Other information sources were not explored because they are considered "less rated". In addition, only scientific articles were selected to conduct the study. Reports, e-books, encyclopedias and invention patents were not explored in the present research. This state of affairs constitutes a limitation for the completeness of the systematic literature review.

6. Discussion

Document exploration reveals the existence of seven categories of bank fraud. The majority of contributions deal with bank credit card fraud, representing 53% of the documents eligible for the study. The XGBOOST-ADASYN model presents the best performance for combating bank credit card fraud. The HFS-LGBM algorithm, based on machine learning, proves effective in solving the problem of identity fraud. The XGBoost Graph Learning model, a hybridization between supervised and unsupervised learning, seems suitable for solving the problem of money laundering in banking institutions. The optimized XGBoost model is more suitable for solving the problem of internal fraud.

Considering the seven types of fraud identified, the result is only a picture reflected by all the documents deemed eligible for the systematic literature review. It is at odds with reality. To the different categories of fraud identified above, we must add check fraud, bank transfer fraud, and cryptocurrency fraud. The list is not exhaustive because criminals are perpetually looking for innovative techniques to accomplish their dirty work. The virtual non-existence of AI-based solutions for these types of fraud can be justified by three hypotheses: (I) traditional solutions manage to effectively detect these categories of fraud, (II) these frauds do not represent a major threat to the banking sector; therefore, they are not a priority for research; (III) these fraud techniques are new and AI-based solutions are currently being developed. The reasons are multiple and may vary depending on several parameters. However, bank credit card fraud occupies an important place in this ecosystem.

The literature shows that the majority of contributions deal with bank credit card fraud, representing 53% of the documents eligible for the study. This is obvious, given the popularity and ease of implementation of this form of fraud. Bank cards of dubious origins are available on the darknet, particularly via specifically dedicated marketing platforms. Anyone eager for easy money can obtain them cheaply and in record time. Moreover, they are reliable. It should be noted that this form of fraud thrives more in developed or developing economies where annual growth is strong. Given the scale of the financial damage it causes, bank credit card fraud is the subject of particular attention in the scientific research community. Several solutions based on AI techniques exist, and the results are convincing.

The best-suited algorithm for solving the credit card fraud problem is XGBoost -ADASYN. It has the best performance in combating this category of fraud. Furthermore, the HFS-LGBM and XGBoost graph learning models are respectively suitable for solving identity theft and money laundering problems in banking institutions. The results are consistent with similar research conducted in a different setting than this article.

7. Conclusion

In conclusion, the banking sector is constantly threatened by fraud of all kinds. It is necessary for banking sector stakeholders, IT security experts, and scientists to have a recent synthesis of previous work to promote a prompt response to threats. This study has examined and identified effective AI techniques against each category of fraud.

The study reveals that the XGBoost -ADASYN model has the best performance in combating bank credit card fraud. The HFS-LGBM technique, based on machine learning, is effective in solving the problem of identity fraud. The XGBoost graph learning model, a hybridization between supervised and unsupervised learning, is suitable for solving the problem of money laundering in banking institutions.

Note that this contribution is a qualitative analysis of the documents studied. It follows a quantitative analysis conducted earlier. Future research should focus on solving the problem of fraud by hybridizing technologies and developing real-time detection techniques.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] Smiles JA, Sasi Kumar A. Synthetic minority oversampling and smote regularized deep autoencoders neural network techniques for fraud prediction in financial payment services. Int J Innov Technol Explor Eng. 2019 ;8 (12):3908 - 15.

[2] Yang Y, Yin Z. Resilient Supply Chains to Improve the Integrity of Accounting Data in Financial Institutions Worldwide Using Blockchain Technology. INTERNATIONAL JOURNAL OF DATA WAREHOUSING AND MINING. 2023 ;19 (4).

[3] Mishra S. Exploring the Impact of AI-Based Cyber Security Financial Sector Management. APPLIED SCIENCES-BASEL. May 10, 2023 ;13 (10).

[4] Dalal S, Seth B, Radulescu M, Secara C, Tolea C. Predicting Fraud in Financial Payment Services through Optimized Hyper-Parameter-Tuned XGBoost Model. MATHEMATICS. Dec 2022;10(24).

[5] Du H, Lv L, Wang H, Guo A. A novel method for detecting credit card fraud problems. Flight. 19, PLOS ONE. 1160 BATTERY STREET, STE 100, SAN FRANCISCO, CA 94111 USA: PUBLIC LIBRARY SCIENCE; 2024.

[6] Ileberi E, Sun Y. Advancing Model Performance With ADASYN and Recurrent Feature Elimination and Cross-Validation in Machine Learning-Assisted Credit Card Fraud Detection: A Comparative Analysis. IEEE ACCESS. 2024 ;12:133315 - 27.

[7] Jovanovic D, Antonijevic M, Stankovic M, Zivkovic M, Tanaskovic M, Bacanin N. Tuning Machine Learning Models Using a Group Search Firefly Algorithm for Credit Card Fraud Detection. MATHEMATICS. July 2022;10(13).

[8] Sasikala G, Laavanya M, Sathyasri B, Supraja C, Mahalakshmi , Mole S, et al. An Innovative Sensing Machine Learning Technique to Detect Credit Card Frauds in Wireless Communications. WIRELESS COMMUNICATIONS & MOBILE COMPUTING. June 23 , 2022 ;2022 .

[9] Palivela H, Rishiwal V, Bhushan S, Alotaibi A, Agarwal U, Kumar P, et al. Optimization of Deep Learning-Based Model for Identification of Credit Card Frauds. IEEE ACCESS. 2024 ;12:125629 - 42.

[10] Salam M, Fouad K, Elbably D, Elsayed S. Federated learning model for credit card fraud detection with data balancing techniques. NEURAL COMPUTING & APPLICATIONS. Jan 20, 2024;

[11] Sharma P, Banerjee S, Tiwari D, Patni J. Machine Learning Model for Credit Card Fraud Detection- A Comparative Analysis. INTERNATIONAL ARAB JOURNAL OF INFORMATION TECHNOLOGY. Nov 2021;18(6): 789-96 .
[12] Ileberi E, Sun Y, Wang Z. Performance Evaluation of Machine Learning Methods for Credit Card Fraud Detection Using SMOTE and AdaBoost . IEEE ACCESS. 2021 ;9:165286 - 94.
[13] Adil M, Zhang Y, Jamjoom M, Ullah Z. OptDevNet : An Optimized Deep Event-Based Network Framework for Credit Card Fraud Detection. IEEE ACCESS. 2024 ;12:132421 - 33.
[14] Estrela P, Albuquerque R, Amaral D, Giozza W, de Sousa RJ. A Framework for Continuous Authentication Based on Touch Dynamics Biometrics for Mobile Banking Applications. SENSORS. June 2021;21(12).
[15] Logeswari G, Bose S, Anitha T. An Intrusion Detection System for SDN Using Machine Learning. INTELLIGENT AUTOMATION AND SOFT COMPUTING. 2023 ;35 (1): 867-80 .
[16] Raza A, Munir K, Almutairi M. A Novel Deep Learning Approach for Deepfake Image Detection. APPLIED SCIENCES-BASEL. Oct 2022;12(19).
[17] Karim M, Hermsen F, Chala S, De Perthuis P, Mandal A. Scalable Semi-Supervised Graph Learning Techniques for Anti Money Laundering. IEEE ACCESS. 2024 ;12:50012 - 29.
[18] Labanca D, Primerano L, Markland -Montgomery M, Polino M, Carminati M, Zanero S. Amaretto: An Active Learning Framework for Money Laundering Detection. IEEE ACCESS. 2022 ;10:41720 - 39.
[19] Karim M, Hermsen F, Chala S, De Perthuis P, Mandal A. Scalable Semi-Supervised Graph Learning Techniques for Anti Money Laundering. IEEE ACCESS. 2024 ;12:50012 - 29.
[20] Hamal S, Senvar O. Comparing performances and effectiveness of machine learning classifiers in detecting financial accounting fraud for Turkish SMEs. INTERNATIONAL JOURNAL OF COMPUTATIONAL INTELLIGENCE SYSTEMS. 2021 ;14 (1):769 - 82.
[21] Asmar M, Tuqan A. Integrating machine learning for sustaining cybersecurity in digital banks. HELIYON. Sep 15, 2024 ;10 (17).
[22] Kotios D, Makridis G, Fatouros G, Kyriazis D. Deep learning enhancing banking services: a hybrid transaction classification and cash flow prediction approach. JOURNAL OF BIG DATA. Oct 2, 2022;9(1).