Cogent Business & Management

ISSN: 2331-1975 (Online) Journal homepage: www.tandfonline.com/journals/oabm20

Comparative analysis of machine learning models for the detection of fraudulent banking transactions

Pedro María Preciado Martínez , Ricardo Francisco Reier Forradellas, Luis Miguel Garay Gallastegui & Sergio Luis Náñez Alonso

To cite this article: Pedro María Preciado Martínez , Ricardo Francisco Reier Forradellas, Luis Miguel Garay Gallastegui & Sergio Luis Náñez Alonso (2025) Comparative analysis of machine learning models for the detection of fraudulent banking transactions, Cogent Business & Management, 12:1, 2474209, DOI: 10.1080/23311975.2025.2474209

To link to this article: https://doi.org/10.1080/23311975.2025.2474209

Published online: 08 Mar 2025.

COGENT BUSINESS & MANAGEMENT
2025, VOL. 12, NO. 1, 2474209
https://doi.org/10.1080/23311975.2025.2474209

BANKING & FINANCE | RESEARCH ARTICLE

OPEN ACCESS Check for updates

Comparative analysis of machine learning models for the detection of fraudulent banking transactions

Pedro María Preciado Martínez[a], Ricardo Francisco Reier Forradellas[b], Luis Miguel Garay Gallastegui[c] and Sergio Luis Náñez Alonso[b]

[a]Technology and Innovation Unit, Caja Rural de Almendralejo SCC, Badajoz, Spain; [b]DEKIS Research Group, Department of Economics, Faculty of Social and Legal Sciences, Catholic University of Ávila, Avila, Spain; [c]UNIR - International University of La Rioja, Logroño, Spain

ABSTRACT

This research presents a comparative analysis of machine learning models for detecting fraudulent banking transactions, a growing problem in the digital financial sector. The aim is to evaluate and determine the most effective model for identifying suspicious transactions, overcoming the challenge of a highly imbalanced dataset. Using data from 565,000 real-world transfers, models based on algorithms such as Random Forest, Neural Networks and Naive Bayes were built and tested. Of these, the Random Forest model proved to be the most robust, achieving 100% accuracy for legitimate transactions and 95.79% accuracy for fraud detection. This level of accuracy reinforces its viability for implementation in real-time banking systems. This result underlines the feasibility of integrating such a model into banking systems for real-time analysis, allowing the interception of dubious transactions. This capability would drastically reduce exposure to financial fraud, optimizing transaction security without compromising operational fluidity. In addition, limitations were identified and future approaches discussed, including oversampling techniques and adjusting class weights to improve detection in unbalanced datasets.

ARTICLE HISTORY
Received 29 August 2024
Revised 21 February 2025
Accepted 25 February 2025

KEYWORDS
Banking industry; bank transfers; fraud detection; risk; machine learning models; Random Forest algorithms; Neural Networks

SUBJECTS
Finance; Artificial Intelligence; Algorithms & Complexity

JEL CLASSIFICATION
G17; G21; C81; C63

Introduction

Technological transformation has led to a new economic paradigm that affects almost all industries (Stiglitz, 2017). Within this process, financial institutions are among the greatest exponents. The financial sector, and more specifically, the banking sector, has led this technological revolution (Cuadros-Solas, 2019). Since the early seventies of the last century, the financial sector began to progressively mechanize its internal operations, resulting in a constant evolution process. Relevant events in this process include the introduction of ATMs in the 1980s, the appearance of online banking at the end of the 1990s, and the adoption of mobile banking with the development of smartphones at the end of the first decade of this century (Afriyie et al., 2023).

However, it is from the global process of digital transformation that the traditional relationship between customers and financial institutions is drastically changed (Coyle, 2016). This process has given rise to new services and business models leading to a real disruption in the structure of the financial services market, giving rise to a *new banking technology* (Toloba & Del Río, 2020). This structural change is a major technological advancement that has allowed the sector to reshape (Arner et al., 2016; Ferrari, 2016). With these advances, one could point to broadband networks and smart mobile devices, cloud computing services, and the exploitation of large amounts of data through big data, artificial

CONTACT Sergio Luis Náñez Alonso sergio.nanez@ucavila.es DEKIS Research Group, Department of Economics, Faculty of Social and Legal Sciences, Catholic University of Ávila, Avila, Spain

intelligence, and blockchain are major factors. This global process has led to a real change in the relationship model that financial institutions currently have with their customers and users. The increase in banking operations through the Internet has increased exponentially because of the facilities offered by new channels. There has been a movement toward a demonetized society where digital payments have become the preferred means of payment, and where the relationship with the bank is mostly in an online format (Carbo-Valverde et al., 2020).

At the same time, this new reality has put the online financial system in the sights of numerous hacker and cybercriminal groups. Undoubtedly, the new form of relationship between the customer and the financial institution has increased the number of intermediaries, which contributes to dilute the direct relationship between the two and to the appearance of security breaches (González-Páramo, 2017). A decade ago the main cases of fraud (more than 60%); were centered on phishing - a technique that passes off a malicious website as an authentic one to trick the victim into providing passwords or performing actions believing them to be legitimate - and malware - viruses, Trojans, and all kinds of programs that run on the victim's computer or mobile (Zieni et al., 2023). Financial institutions today face a steady increase in attacks due to increasingly sophisticated cybercrime (Akinbowale et al., 2020; Al-Surkhi & Maqableh, 2024; Zieni et al., 2023). One of the targets sought by these cybercriminals are bank transfers, which number in the millions every day, and their number is steadily increasing. Sending fake wire transfers has become a lucrative business for these criminal groups, which banks must constantly fight against to avoid bankruptcy and not cause distrust among their customers (Abdul Rani et al., 2024; Tambe Ebot, 2023). According to Mangala and Soni (2023), fraud in the banking sector worldwide has become a major concern. This study puts wire transfer fraud at approximately 0.172% of total transactions. It is thus a global phenomenon that affects both developing countries such as Nigeria, as shown by the study of Odukoya and Samsudin (2021) or India according to the study of Sharma and Sharma (2018). But developed countries are not exempt from this type of cybercrime either. Thus, we find the existence of this phenomenon at the European level in the study by Ramos et al. (2024); as well as in some European countries such as Spain in the study by Kemp et al. (2020). Also, in the study by Mangala and Soni (2023) the concern about fake bank transfers in the U.K., Greece, Spain, Italy and Germany is analyzed. On the African continent, there are also studies such as that of Phiri et al. (2024); which show concern about this type of fraudulent bank transfers. Or also, in the American continent, with the study by Paraná (2024) in Brazil. However, within the total number of bank transfers, it can be difficult to differentiate between those with a criminal purpose and those that are legitimate (European Banking Authority, 2021). In addition, techniques to detect these transactions are time-consuming and error prone. Having a machine learning mechanism that analyzes these transactions will reduce human intervention, minimize detection errors, and ensure scalability in the face of increased transactions (Detthamrong et al., 2024; Jiao & Li, 2023), whether unsupervised or supervised models (Afriyie et al., 2023; Detthamrong et al., 2024).

The main objective of this research is to evaluate different machine learning models for real-time identification of fraudulent banking transactions. Given the growth of digital transactions and the increase in financial fraud, our study focuses on identifying the model that offers the highest accuracy and robustness for implementation in banking systems. In particular, we seek to determine the most effective model under conditions of unbalanced data, where legitimate transactions greatly outnumber fraudulent ones. As the model is trained on historical fraud-related data, it can distinguish between usual and potentially suspicious behaviors. Consequently, it can assess in real time whether a transaction, whether common or unusual, has a high probability of being fraudulent, giving it a fraud score. In our research, to define the model, K Nearest neighbors, naive Bayes, support vector machines, random forest, and neural network algorithms were compared. In view of these results, we determined that the best model would be Random Forest. This model, after being tested with data from 141,174 transfers (141,079 were legitimate and 95 fraudulent), successfully identified 100% of the former, being wrong only in four cases of fraud that could not be detected, i.e. 95.79% of fraud cases detected.

The article is structured as follows: The Introduction presents the problem of fraud in banking transactions and the need to apply machine learning techniques. The Literature Review explores previous research and technical challenges, such as data imbalance. The Materials and Methodology section describes the dataset and models evaluated, such as Random Forest and neural networks, explaining the evaluation metrics employed. The Results highlight the effectiveness of Random Forest in identifying fraud. The

Discussion discusses possible improvements, such as oversampling techniques. Finally, the Conclusions confirm the feasibility of Random Forest and suggest future research, including the use of blockchain.

Literature review

Traditionally, audit teams in different financial institutions have used manual techniques to detect fraud (Qawqzeh & Ashraf, 2023), a process that is slow, costly, inaccurate and impractical. The sophistication and diversity of fraudulent techniques have rendered traditional rule-based fraud detection approaches increasingly ineffective (Minastireanu & Mesnita, 2019).

All financial institutions are aware that one of the main problems they face today is due to the exponential increase in financial cybercrime (Akinbowale et al., 2020). The exponential increase in the use of wire transfers has also meant an increase in the same proportion in fraud attempts linked to these operations (Al-Surkhi & Maqableh, 2024; Zieni et al., 2023). The similarity between fraudulent and legitimate banking transactions presents a major challenge to current fraud detection techniques (Amasiatu & Shah, 2018; Krishna et al., 2023; Wickramanayake et al., 2020). Researchers and industry experts have turned to advanced machine learning techniques, harnessing the power of data mining and artificial intelligence to developmore robust and adaptive fraud detection systems (Detthamrong et al., 2024). In search of efficiency, machine learning and deep learning tools have been used to automate these processes and reduce detection time.

In this sense, this massive growth in the use of banking transactions makes the application of informatics tools essential for effective fraud detection. However, as will be shown in this paper, the key factor affecting the quality of a fraud detection system is how to extract useful features from transaction attributes (Cui et al., 2021). It seems clear that there is no doubt in academia about the need to apply new computational tools in the fight against bank fraud, and it is precisely how to apply these techniques that is the subject of debate in the scientific arena. In fact, the limitations of the existing body of academic work will be defined by the correct construction of a model that can handle efficiently and with the least margin of error an unbalanced data set (Alshameri & Xia, 2023). To overcome these limitations, the present work is based on studies already carried out and allows improving the existing results by having a model trained with more than 565,000 real transactions -complying with all aspects related to customer data protection- and with a higher hit rate than the rest of the models, as will be shown in the conclusions section.

For decades, several authors have highlighted the possibility offered by Machine Learning techniques to quickly detect situations that differ from the usual behavior of financial users, which may indicate possible cases of fraud and the possibilities offered by machine learning in the identification of fraudulent activities in general terms and specifically in payment systems (Phua et al., 2005).

A study developed in 2016 predicted that artificial intelligence and machine learning applications would dictate how banks interact with their customers in the near future (Purdy & Daugherty, 2016). Bank transfers are one of the fundamental pillars on which the banking business is based and are counted by millions on a daily basis (Mehdiabadi et al., 2020) so the importance and relevance of the line of research to be pursued in the present work is beyond doubt, as it is a fully accepted issue in academia (Borketey, 2024). Bank transfers have grown exponentially in the digital world, and fraud has been linked to these transactions (Azhar et al., 2020; Mangala & Soni, 2023). This is why the banking sector is one of the sectors where artificial intelligence can find greater application (Rahman et al., 2023). Thus, the advancement of Artificial Intelligence (AI), machine learning and data mining has been used to detect and predict these fraudulent activities in the financial sector, both through supervised and unsupervised methods (Ali et al., 2022). These new approaches have the potential to work with large amounts of real transaction data, making it possible to uncover complex patterns of behavior and adapt to the constantly evolving tactics employed by fraudsters (Manikandaprabhu et al., 2023).

It should be noted that in the financial sector, competition is intense, profit margins shrink, and electronic transactions increase at an unbridled pace. Machine Learning, as a branch of Artificial Intelligence, provides fraud detection managers with real-time risk scores and a broader perspective on where to define scoring thresholds to optimize sales and minimize losses due to fraud by establishing models that make decisions using intelligent algorithms (Vergara et al., 2024). With the use of artificial intelligence, a

bank can expect potential savings of 20–25 percent in IT operations, including infrastructure, maintenance, and development costs (Jubraj et al., 2018). Similarly, one of the main contributions of machine-learning techniques in the sector is linked to security aspects allowing processes to become increasingly intelligent and automatic (Hans, 2016; Vergara et al., 2025). A machine-learning mechanism that analyzes these transactions reduces human intervention and ensures scalability (Liu et al., 2020). Bolton and Hand developed in their early work the possibility offered by machine learning to provide useful predictions and correlations when detecting fraudulent financial activities (Bolton & Hand, 2002).

However, predicting fraudulent transfers entails serious difficulties. On one hand, the amount of data to be analyzed is very large, so the model must have a fast response capability to handle requests over time (Ali et al., 2022; Arfeen & Khan, 2023; Cherif et al., 2023). However, the data with which the model should be trained is not balanced (Alfaiz & Fati, 2022; Al-Hashedi & Magalingam, 2021; Gupta, 2023). Added to addition, most of the transfers made are legitimate (possibly less than 0.01% are scams (Arfeen & Khan, 2023). Therefore, it may be difficult to detect these cases. Finally, the information to be analyzed contains personal data; therefore, it is necessary to respect data protection throughout the process (Ali et al., 2022; Al-Hashedi & Magalingam, 2021; Cherif et al., 2023). To answer the final objective of the work, it will be necessary to develop a simple and fast model with a fraud-detection engine that can provide an acceptable answer in the shortest possible time. The Random Forest model (combination of decision trees) is the model of choice because it has a high degree of accuracy and good performance when the amount of data to be used is high (Wang et al., 2020). In the academic field, several authors bet on this algorithm in systems for bank fraud detection, such as the models proposed by Liu et al. (2015) or Sohony et al. (2018).

One of the main problems raised by academia when analyzing a set of bank transfers to detect possible fraud is the so-called data imbalance. As noted above, the vast majority of wire transfers are legitimate. This imbalance in the data (unbalanced data) can constitute a drawback in model building, as it becomes more difficult to detect patterns when there are few records in the minority class (Kubat & Matwin, 1997).

To provide mechanisms to address the problem of unbalanced data, various authors have worked on similar models have been followed (Alfaiz & Fati, 2022; Al-Hashedi & Magalingam, 2021; Analytics Vidhya, 2016) or (Gupta, 2023). As noted above, the vast majority of bank transfers are legitimate. This imbalance in the data (unbalanced data) can constitute a drawback in model building, as it becomes more difficult to detect patterns when there are few records in the minority class (Kubat & Matwin, 1997).

The most common mechanisms to address the problem of unbalanced data are as follows, as indicated by various authors, such as Analytics Vidhya (2016), Alfaiz and Fati (2022), Al-Hashedi and Magalingam (2021), and Gupta (2023). First, there is one-way under sampling. According to Dong et al. (2021), this consists of decreasing the majority class and increasing the minority class size. The disadvantage could be that information can be lost by reducing the number of observations. Second, oversampling. According to Liu et al. (2019), the aim is to replicate observations of the minority class to achieve better data balancing. New replicates can be added either randomly or by following specified criteria. Although the algorithm performed well on training data, it performed worse on real data. Third, the Synthetic Minority Oversampling Technique (SMOTE) was used for synthetic data generation. According to Chawla et al. (2002), this technique consists of using an algorithm based on KNN (K Nearest Neighbors) to add artificial data to the minority class. Fourth, the combination of under sampling and oversampling was indicated by Analytics Vidhya (2016), Dong et al. (2021), and Liu et al. (2019).

The main factors that determine the choice of machine learning algorithm to be used depend on the high predictive capability and speed of the model performance. The Random Forest model is going to be a good candidate to consider and is chosen by many authors in academia to implement fraud detection systems in other domains (Liu et al., 2015; Sohony et al., 2018). Authors such as Pal also defend the advantages of using the Random Forest method in similar studies over other models by demonstrating that the number of user-defined parameters required by the Random Forest model is lower than that of similar models (Naive Bayes or Support Vector Machine) and easier to define (Pal, 2005). Authors such as Dávila, Castillo-Sáenz, and Vargas-Murillo, in their studies on the application of machine learning models in the detection of fraud in financial transactions, concluded that the Random Forest model was the most effective (0.956) for accurate fraud detection in real time (Dávila-Morán et al., 2023). Authors defended in their work that better results were granted by this type of model than others based on Naive Bayes when predicting in the best way

fraudulent transactions from non-fraudulent ones. Similarly, in academic works such as that of Campus (2018) the application results of Random Forest models obtained values of 0.975 when analyzing the dataset with financial transactions (bank cards in this particular case), above other models such as Support Vector Machines that obtained values close to 0.955. Likewise, similar studies (Mytnyk et al., 2023) indicate that the logistic regression algorithm obtained the best results, with an AUC value of approximately 0.946.

Logically, the use of Machine Learning techniques as a basis for detecting possible fraudulent transactions has already been implemented in the financial system itself. The Spanish financial institution BBVA (Banco Bilbao Vizcaya Argentaria), together with MIT (Massachusetts Institute Technology), introduced a model based on Machine Learning-based algorithms to reduce by 54% the results erroneously classified as fraudulent in credit card transactions. According to the Gini index (developed by the World Bank to measure various indicators via data and surveys), the implementation of Machine Learning techniques increases to more than 90% the accuracy of prediction in the decisions implemented (compared to the traditional 50–60%), which means a considerable decrease in the risk derived from fraudulent transactions. Some examples of models based on Machine Learning techniques for the detection of fraudulent transactions similar to what we intend to provide in this work are the work of Santamaría Ruíz, (2010) where a multilayer perceptron neural network was used to define patterns associated with fraud in bank transfers; from (Dhankhad et al., 2018) where supervised machine learning algorithms are proposed to detect fraudulent credit card transactions; from (Yee et al., 2018) where Machine Learning techniques are used to predict suspicious and non-suspicious transactions automatically by using classifiers; from (Campus, 2018) where raw data and pre-processed data are applied on bank fraud data through different Machine Learning models; from Vergara et al. (2025) which used specific anomaly and fraudulent pattern detection algorithms through various classification, regression and clustering techniques; Ileberi et al. (2022) proposes predictive analytics methodologies based on Random Forest with the aim of predicting future events - in this case fraudulent transactions - as accurately as possible; (Sailusha et al., 2020) implemented learning algorithms for fraud detection in financial transactions linked to credit cards by comparing the results of various algorithms.

However, in the present work, we compare the results offered by Random Forest against other alternatives, such as Naive Bayes (Chen et al., 2020), k-nearest neighbors (Papernot & McDaniel, 2018), Support Vector Machines (Chauhan et al., 2019) or synthetic minority oversampling techniques (Alshameri & Xia, 2023). With this literature review, it seems clear that artificial neural networks, particularly deep learning algorithms, have proved to give very satisfactory results in finding hidden and complex relationships in large datasets and in their application to the study of fraudulent banking transactions (Bello et al., 2024).

The limitations of the different works studied in the literature review will be defined by the structure and volume of the data used in the sampling, as well as the tools used in the data balancing. The accuracy of the model may be compromised by incomplete and insufficiently diverse data sets, which may lead to false positives. Another limitation is the possibility of human bias in data selection and analysis, which may affect the validity and reliability of the method. On the other hand, it is important to avoid overfitting, i.e. that the model performs well on the training data set but poorly on the test data set due to its complexity and limited generalizability.

The model proposed in the present work attempts to overcome the above limitations. By developing a robust artificial neural network, the accuracy in detecting fraudulent transactions is significantly increased. With the set of real transactions used as the source of the model, a 100% success rate in the detection of non-fraudulent transactions is achieved, which avoids working with false positives. The work provides methods to improve detection accuracy, as well as to improve the management of unbalanced data sets, feature transformation, and feature engineering.

The literature review itself suggests that for future research it would be interesting to incorporate, in addition to the application of Machine Learning and Artificial Intelligence techniques, blockchain technology as a new way to prevent banking fraud (Mytnyk et al., 2023).

Materials and methodology

Materials

Real data on standard bank transfers were collected to develop the proposed model. The Dataset comprised 565,000 records of actual wire transfers made between 1/01/2024 and 11/02/2024. The bank

transfer data in the dataset contains personal information that will be protected by national or international data protection laws, such as the European GDPR. Thus, to make use of the data in our analysis, we have resorted to the technique pointed out by Jain and Puri (2020), Reier Forradellas et al. (2020), and Garay Gallastegui et al. (2024), called 'masking of sensitive fields'. However, this dataset can be downloaded upon request from the authors of this study.

In the dataset used, the number of legitimate transfers was 564,326 and the number of fraudulent transfers was 333. This makes a ratio of 0.059%. The number of fraudulent transfers was €45,174, which highlights the need for a mechanism to curb these criminal operations. Each transfer was stored in a database. Table A1 in the appendix describes the fields that make up these records and their 'masking'. Due to privacy reasons and in compliance with GDPR, sensitive personal information was masked in the data collected as indicated above. According to Jain and Puri (2020), Reier Forradellas et al. (2020) or Garay Gallastegui et al. (2024), the actual data to be masked have been replaced by numerical identifiers, so that the same data 'X' is always matched with the same identifier 'N', thus preserving the integrity and reliability of the analysis.

Figure 1 shows the distribution of bank transfers by amount, broken down into four distinct histograms to provide a detailed view of different ranges. Specifically, panel (a) presents the complete distribution of all transfers, without separating them by amount, offering a comprehensive overview of the overall distribution; panel (b) focuses on small bank transfers of less than €1,000, capturing the most frequently occurring transactions within this lower range; panel (c) displays transactions between €1,000 and €10,000, where a gradual decrease in frequency is observed as the transaction amount increases; and panel (d) shows those exceeding €100,000, illustrating the lowest volume of transactions, as higher amounts are less common.

This subdivision facilitates a detailed analysis of transfer behavior across different monetary ranges and highlights patterns such as the frequent use of round figures and the lower occurrence of high-value transfers.

So, Figure 1 shows that the most frequent bank transfers are within the range of €0 to €100. Additionally, slight increases in the distribution can be observed when amounts are rounded numbers, such as €200, €400, €500, and €1,000, indicating a potential preference for specific transaction values. For amounts greater than €5,000, the number of transfers is significantly lower, reflecting the rarity of higher-value transactions in the dataset.

Exploration of the data showed that the information was consistent. No errors, missing data, outliers, or sentinel values were observed. This figure has been incorporated in a more developed way since it is important to know the structure of the data to be used in order to later validate the system based on unbalanced data. Considering this normal distribution of transactions, both in specific imports and in volume, the model can be trained to have a higher percentage of validity in the predictions.

Methodology

Our study focuses on the development of a mechanism based on artificial intelligence (machine learning) for the detection of suspicious bank transfers. Figure 2 illustrates the stages in the methodology used for detecting suspicious bank transfers. The process is divided into three main phases: Data Preparation, Application of Classification Models, and Model Training and Testing. The Data Preparation phase includes data extraction, attribute selection, data cleaning, and anonymization. The Application of Classification Models phase involves applying machine learning algorithms, such as K-Nearest Neighbors, Naive Bayes, Support Vector Machines, Random Forest, and Neural Networks. Finally, the Model Training and Testing phase evaluates model performance through metrics like Accuracy, Precision, Recall, F1 Score, and Matthews Correlation Coefficient (MCC), as well as using a confusion matrix to analyze True Positives, False Positives, True Negatives, and False Negatives.

First, we extracted relevant data for model training. Subsequently, a data preparation phase is conducted that involves the elimination of irrelevant attributes, creation of new attributes if necessary, and elimination of invalid or incorrect data that may affect model performance (Sharma & Yadav, 2021). In addition, anonymization and masking techniques have been implemented to ensure the privacy and confidentiality of sensitive data (Jain & Puri, 2020; Reier Forradellas et al., 2020). Identifiable information,

such as account identifiers and transaction participant details, was anonymized through hashing and encoding methods, replacing original values with unique codes to maintain data integrity without exposing personal information. The fields or features removed are listed in Table A2 of the Appendix. These are a series of fields of no interest in the study because they are variables used internally by the bank.

For the correct design of the machine learning algorithm, certain data that are not initially collected in the records of the transfers issued (creation of attributes) will be useful. The relevant data will be the total sums or percentages that allow discrimination between possible fraudulent transactions and those that are not. Using a batch program launched within the entity, a feature engineering process was carried out to calculate and add to each observation of the dataset the characteristics (features) related to the transfers issued and those related to the beneficiary accounts (Garay Gallastegui et al., 2024; Poudel et al., 2024).

Before building the model, it was necessary to prepare the data and normalize the attributes. Data preparation involves transforming text-type categories into numerical categories, which are more appropriate for use in machine learning algorithms. Thus, a column containing text type values such as 'Badajoz', 'Madrid', 'Ávila', etc. -referring to cities of origin of the transfers- will be encoded as a sequence of numbers: '1', '2', '3', etc. This transformation was performed using the LabelEncoder package of the sckit-learn library.

After data preparation, the dataset was divided into a training set (75% of the data) and a testing set (25% of the data) to evaluate model performance, ensuring that all validation was conducted solely on the original dataset. This split ratio ensures that the model is trained with sufficient data and that a separate subset is retained to validate its effectiveness. The training data was used to build and fine-tune the model, while the testing data provided an unbiased evaluation of its performance on unseen data. No external datasets were used in this study, as the split was designed to provide balanced and reliable validation directly from the data collected.

As the dataset contains numerical features with varying scales, normalization was applied to ensure consistency across all attributes. The StandardScaler from scikit-learn was used to transform the values of each numerical attribute to a standard scale with a mean of 0 and a standard deviation of 1. This scaling process is crucial for certain machine learning algorithms, such as Support Vector Machines and Neural Networks, which are sensitive to the scale of input features. Table 3 in the appendix shows the final columns of the final dataset on which the model was built.

Second, several classification models based on machine learning have been explored, and the model is trained with 423,521 transactions and tested with 141,174 samples by applying the following algorithms: K Nearest neighbors (Papernot & McDaniel, 2018), Naive Bayes (Chen et al., 2020); Support Vector Machines (Chauhan et al., 2019), Random Forest (Liu et al., 2015; Sohony et al., 2018); and Neural Networks. Each model was evaluated in terms of its ability to identify suspected fraud cases after appropriate training. Evaluation metrics were defined to assess model performance: Accuracy, Recall, F1 Score, and the Matthews Correlation Coefficient (MCC) (Chicco et al., 2021).

Third, we trained and tested the selected models. During this stage, the performance of each model is evaluated using the metrics defined above. A confusion matrix was used to visualize the model performance. Four data points were used for this purpose: 1. True Negative (TN). This number is equivalent to the number of legitimate transfers detected. False-positive (FP). These are legitimate transfers that the algorithm identifies as fraudulent. False-negative (FN). It includes fraudulent transfers detected as legitimate. 4. True Positive (TP). These are fraudulent cases correctly detected by the algorithm.

Results

The main objective of our study was to provide a system to distinguish fraudulent transactions from non-fraudulent transactions. Therefore, it is necessary to compare the number and number of legitimate transfers with the number and amount of fraudulent transfers so that we know the proportion. The results are presented in Table 1.

With all of the above data, the model obtains the system correlation matrix shown in Figure 3.

In view of the matrix, it can be deduced that there are no features that significantly affect the target fraud individually, so the model we created identifies fraudulent transactions based on the combination

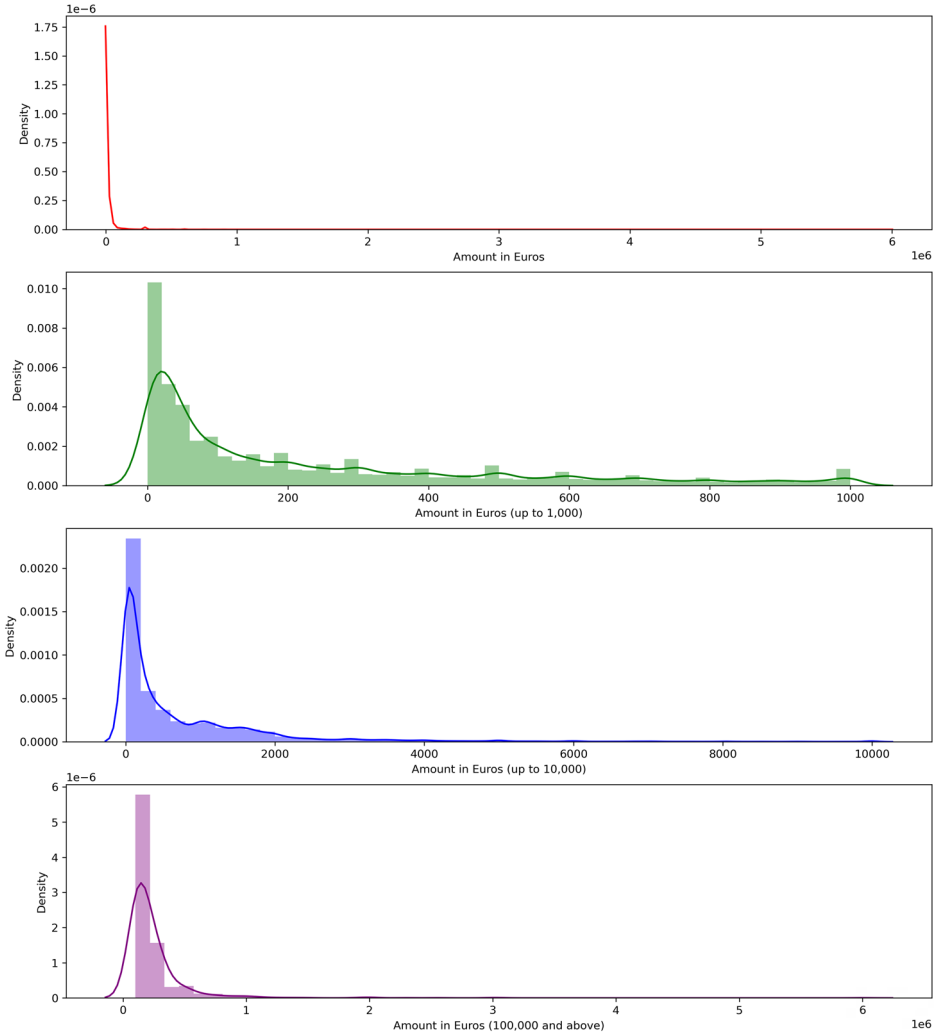

Figure 1. Density Distribution of Bank Transfers by Amount Range: (a) All Transfers, (b) Transfers up to €1,000, (c) Transfers up to €10,000, (d) Transfers of €100,000 and above. *Source:* own elaboration.

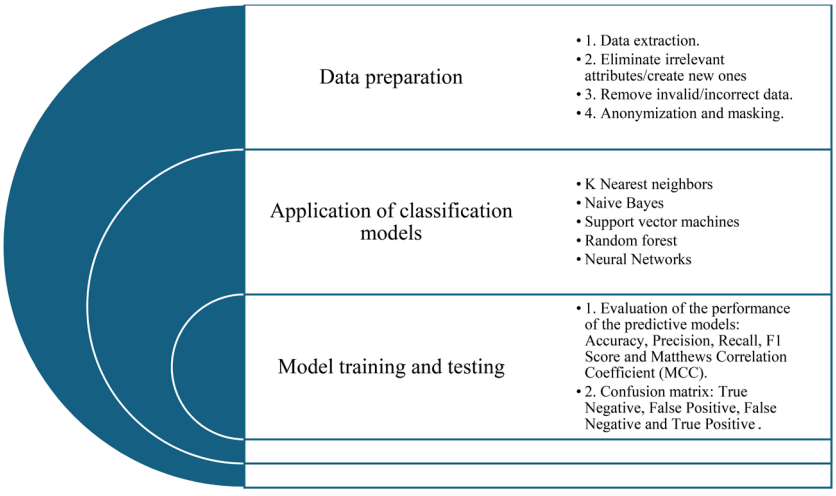

Figure 2. Methodological Workflow for Detecting Suspicious Bank Transfers. *Source:* Own elaboration.

Table 1. Final result of fraudulent and legitimate transactions.

	Number	Percentage	Amount
Legitimate transfers	564362	99,940995	938981066.5800002
Fraudulent transfers	333	0,059005	45174.7399999

Source: Own elaboration based on dataset.

of several or all the available features previously normalized and contained in Table A3 of the Appendix: Final columns of the dataset.

The classification models elaborated with different machine learning algorithms were tested using the dataset reserved for the tests. The results for each algorithm were evaluated based on the metrics presented in Table 2.

Among the models evaluated, Random Forest provided the most robust and accurate results in distinguishing legitimate and fraudulent transactions. This choice of Random Forest was due to its high accuracy in handling imbalanced datasets, which is a common challenge in fraud detection. Random Forest is a supervised learning algorithm that constructs multiple decision trees during training, combining their outputs to improve accuracy and reduce overfitting. This ensemble approach allows it to capture complex patterns within the data, which is crucial in detecting anomalies in highly imbalanced datasets, such as ours. Below is a pseudocode representation of the Random Forest implementation in our research:

1. Import and preprocess the dataset (data cleaning, anonymization, normalization).
2. Split the dataset into training (75%) and testing (25%) sets.
3. Configure the Random Forest classifier with the following parameters:
    - Number of trees (estimators): 10
4. Scale the features using StandardScaler to normalize the values.
5. Train the Random Forest model on the training dataset.
6. Make predictions on the testing dataset.
7. Evaluate model performance using metrics:
    - Accuracy: Proportion of correctly classified transactions.
    - Precision: Proportion of true positives among predicted positives.
    - Recall: Proportion of true positives among actual positives.
    - F1 Score: Harmonic mean of precision and recall.
    - Matthews Correlation Coefficient (MCC): A balanced measure of model accuracy.
8. Generate a confusion matrix to analyze True Positives, False Positives, True Negatives, and False Negatives.

As shown in Table 3, the sample consisted of 141,174 bank transfers. The vast majority of respondents (141,079) were considered legitimate. This means that they represent normal and authorized transactions within the financial system. By contrast, 95 cases of fraudulent transfers were identified in the same dataset. These fraudulent transfers constitute a significant minority compared with legitimate transfers.

Finally, Table 4 presents a comparison of the results of the different confusion matrices generated for each algorithm. Together with the indicators of true positives, false positives, false negatives, and true positives, the percentage of true positives with respect to the real number of legitimate or fraudulent samples was shown.

In view of the results, the most robust model and the one that provided the best predictions were the one based on Random Forest, which performed brilliantly, with a 100% hit rate in the case of legitimate transfers, and four cases of fraudulent transfers identified as good (false negatives), which is equivalent to 95.79% of fraud cases detected.

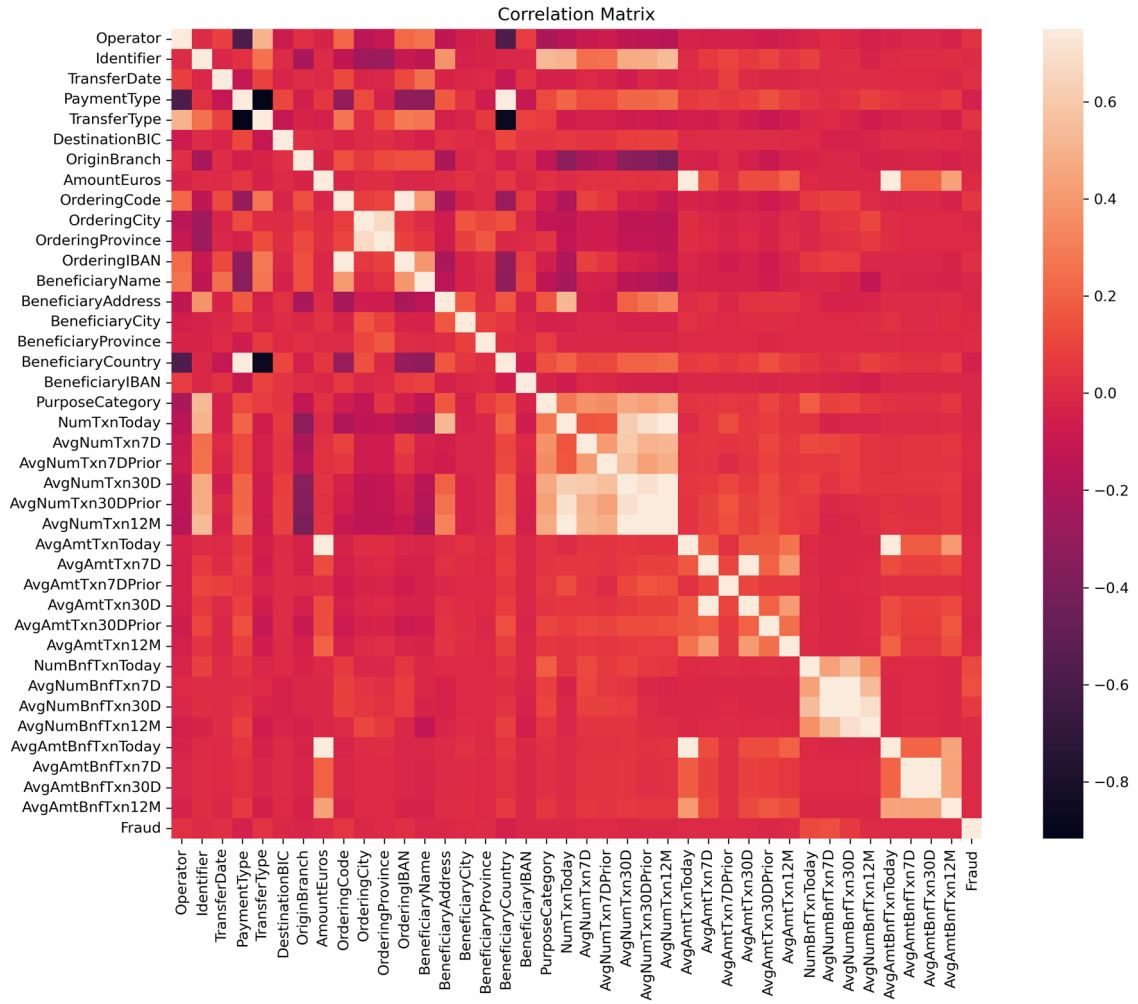

Figure 3. Correlation matrix. *Source:* Own elaboration based on dataset.

Naive Bayes models, however, demonstrated significantly poorer performance. For instance, although Gaussian Naive Bayes detected 98.95% of fraud cases (94 out of 95), it only managed to identify 58.62% of legitimate transfer samples, performing barely better than a random classifier. This outcome is likely due to the data distribution and class imbalance, to which Naive Bayes algorithms are particularly sensitive. Naive Bayes classifiers, which assume independence between features, tend to struggle with imbalanced datasets like this one. The overwhelming prevalence of legitimate transactions biases the model, leading to a high rate of false positives and low precision for legitimate transfers. This poor performance can be attributed to the algorithm's fundamental assumption of feature independence, which does not hold in the dataset used in this study. Specifically, the correlation matrix revealed significant interactions between transaction amount and frequency—patterns that Gaussian Naive Bayes failed to capture. Consequently, the model misclassified legitimate transactions with atypical amounts or frequencies as fraudulent. Furthermore, the model's reliance on Gaussian distributions for numerical features exacerbated this issue, as the presence of skewed distributions distorted the probability estimates. Likewise, Support Vector Machines (SVM) showed a reduction in performance for detecting fraudulent transactions, with only 84.21% of fraud cases correctly identified. SVM, which aims to maximize the margin between classes, faces challenges in accurately identifying the minority class due to the scarcity of positive samples (fraud cases) in the dataset.

To improve model performance, especially for algorithms sensitive to data imbalance, several methods can be considered. One approach is oversampling the minority class. Techniques such as the Synthetic Minority Over-sampling Technique (SMOTE) generate synthetic examples of fraudulent transactions, which help balance the dataset and provide the model with additional information about the minority

Table 2. Metrics calculated from the tests.

	Accuracy	Precision	Recall	F1 Score	MCC
Random forest	0,99997	1,00000	0,95789	0,97849	0,97871
Gaussian Naive Bayes	0,58647	0,00161	0,98947	0,00321	0,03031
Multinomial Naive Bayes	0,79424	0,00306	0,93684	0,00609	0,04684
Bernoulli Naive Bayes	0,99176	0,07074	0,92632	0,13144	0,25476
KNN	0,99996	1,00000	0,93684	0,96739	0,96789
SVM	0,99989	1,00000	0,84211	0,91429	0,91761
Neural Networks	0,99996	1,00000	0,93684	0,96739	0,96789

Source: Own elaboration.

Table 3. Number of actual positive and negative samples in test data.

Number of samples	141.174
Legitimate Transfers (TN)	141.079
Fraudulent transfers (TP)	95

Source: Own elaboration.

Table 4. Test results.

	TN	% TN	FP	% FP	FN	% FN	TP	% TP
Random forest	141 079	100,00	0	0	4	4,21	91	95,79
Gaussian Naive Bayes	82 700	58,62	58 379	41,38	1	1,05	94	98,95
Multinomial Naive Bayes	112 037	79,41	29 042	20,59	6	6,32	89	93,68
Bernoulli Naive Bayes	139 923	99,18	1156	0,82	7	7,37	88	92,63
KNN	141 079	100,00	0	0	6	6,32	89	93,68
SVM	141 079	100,00	0	0	15	15,79	80	84,21
Neural Networks	141 079	100,00	0	0	6	6,32	89	93,68

Source: Own elaboration.

class. This method enhances recall and reduces false negatives, particularly benefiting models like Naive Bayes and SVM.

Another approach is to adjust the class weights. Many algorithms, including SVM and Random Forest, allow for modifications in class weights to assign greater importance to the minority class. By increasing the weight of fraudulent transactions, the model can focus more on detecting fraud, which improves performance metrics such as recall and F1 Score. Lastly, ensemble methods offer a way to counteract the limitations of individual classifiers by combining the predictions of multiple models.

Techniques like boosting, including AdaBoost or Gradient Boosting, can be particularly effective in imbalanced contexts by aggregating weak classifiers to strengthen the overall model, making it more resilient to class imbalance.

As for the rest of the algorithms, KNN, SVM and Neural Networks, it also yielded an optimal result, with the Accuracy, Precision, Recall, F1 Score and MCC metrics close to 1, although perhaps somewhat less favorable in the case of support vector machines. The numbers for KNN and Neural Networks are similar: both algorithms correctly identified 100% of the 141,079 legitimate transfers and missed six of the 95 fraudulent transfers, which equates to a 93.68% hit on true positives (TP). SVM has also achieved a full number of hits on genuine transfers, but has lowered performance in identifying fraud cases, considering 15 out of 95 transfers valid, that were not, i.e. 84.21% correct in predicting fraudulent transfers.

Overall, the models generalized well despite the imbalance of the classes input, and it was not necessary to resort to under sampling or oversampling techniques. The Random Forest model exhibited the best overall performance, with a high accuracy rate and robust performance in detecting fraudulent transactions. By capturing complex patterns in the data, Random Forest minimized both false positives and false negatives, making it a strong candidate for deployment in a production environment. Other models, such as KNN and Neural Networks, also performed well, though slightly less effectively than Random Forest.

The Random Forest demonstrated superior performance in detecting fraudulent transactions, particularly when dealing with a highly imbalanced dataset. This advantage stems from its ensemble of learning architecture, which constructs multiple decision trees and combines their predictions through majority

voting. Unlike algorithms that rely on single-model assumptions, Random Forest leverages the diversity of its trees to reduce variance and mitigate overfitting. Additionally, by randomly selecting subsets of features during tree construction, the model minimizes the risk of irrelevant or redundant predictors dominating the learning process. These mechanisms collectively enhance the model's ability to accurately identify fraudulent transactions, achieving a fraud detection rate of 95.79%, despite the imbalance present in the dataset.

In contrast, Naive Bayes models were more affected by the class imbalance and data distribution, leading to lower accuracy. Overall, the selected models demonstrated strong generalization capabilities, confirming the effectiveness of Random Forest, KNN, and Neural Networks in handling imbalanced datasets without the need for resampling techniques.

Discussion of results

Currently, the rise in online banking fraud poses a significant challenge to global financial security. In the face of this growing threat, banks and financial institutions must implement proactive measures to combat fraud (Azhar et al., 2020; Mangala & Soni, 2023). One of the most effective strategies is the adoption of Machine Learning (ML) systems, predicting and detecting fraudulent transactions early is one of the most effective strategies. Therefore, the timeliness and relevance of this work is beyond any doubt.

However, it is crucial to understand that cyber fraud is a constantly evolving problem, with cyber criminals continually developing and adjusting techniques to circumvent security systems. Therefore, any ML implemented should not be static but should be periodically retrained and calibrated to maintain its effectiveness in the face of new emerging threats (Garay Gallastegui et al., 2024; Reier Forradellas et al., 2020; Sawdatkar et al., 2023). This can also be complemented by sentiment analysis techniques (Garay Gallastegui et al., 2024; Ozili & Alonso, 2024). For this reason, it has been considered appropriate and of scientific interest to present this research, contributing new conclusions and methodologies to the existing broad scientific field.

In the specific case of this research, it is necessary to understand that although fraudulent bank transfers are a minority compared to legitimate ones, the former are of great importance due to the impact they have on the sector. This is because of their potentially negative impact on the security and integrity of the banking system. It is essential to highlight the need for effective fraud detection methods to identify and prevent such cases within a sea of legitimate transactions. As noted in the previous points, the similarity between fraudulent banking transactions and legitimate banking transactions represents one of the main problems in current fraud detection systems (Amasiatu & Shah, 2018; Krishna et al., 2023; Wickramanayake et al., 2020). The main limitation encountered by authors working on these issues lies in defining a model that can efficiently handle an unbalanced data set (Alshameri & Xia, 2023). The model developed in this work is based on studies and articles already published by other researchers. It is a model trained with more than 565,000 real transactions -taken from real data of banking operations between 1/01/2024 and 11/02/2024- with a higher accuracy rate than the rest of the models, as will be shown in the conclusions section. In the dataset used, the number of legitimate transfers was 564,326 and the number of fraudulent transfers was 333. This makes a ratio of 0.059%, data that are in line with the industry average as observed in the literature review.

As demonstrated in the results section, the model that provided the best predictions for the proposed objective was the one based on Random Forest, which performed with a 100% hit rate for legitimate transfers and 95.79% of the detected fraud cases. Comparing the results with those collected in similar academic studies -many of them already referred to in the previous sections–, it can be observed that the model proposed in this study is consistent with the reliability of the results obtained. At the same time, despite being based on machine learning techniques already used in the academic field, the work is relevant, original, robust - since it is based on 565,000 transactions - and makes specific contributions to the state of the art. Among the models evaluated, Random Forest provided the most robust and accurate results in distinguishing legitimate transactions from fraudulent ones. Random Forest was chosen because of its high accuracy in handling unbalanced data sets, which is a common challenge in fraud detection.

In this discussion section it may be interesting to compare the model presented with similar works, many of which have already been mentioned in the literature review. Thus, simply as a summary, we can include the following works carried out by authors who sought similar objectives. Thus, authors such as Dávila-Morán et al. (2023), in their studies on the application of machine learning models in the detection of fraud in financial transactions, trained and optimized models such as Random Forest, Convolutional Neural Networks, Naive Bayes, and Logistic Regression. Among them Random Forest and Convolutional Neural Networks achieved F1 score higher than 95% on average. Random Forest produced the highest average F1 score of 0.956, indicating that the models detected 45% of fraudulent transactions with low variability. The model presented in the present work obtains Random Forest scores of 95.79% for detecting fraudulent transactions (TP) and 100% for detecting legitimate transactions (TN).

Campus (2018) investigated the performance of a decision tree, Random Forest, SVM, and logistic regression on highly skewed credit card fraud data from a credit card transaction dataset containing 284,786 instances. The performance of these techniques was evaluated in terms of accuracy, sensitivity, and specificity. The results indicated that the optimal accuracy for logistic regression, decision tree, Random Forest, and SVM with values of 97.7%, 95.5%, 98.6%, 97.5%, respectively. As can be seen, the data are similar to those obtained in the present study with the difference that the proposed model is trained with more than twice as many bank transactions and that the hit rate for legitimate transactions is 100%.

In addition, Yee et al. (2018) employed machine learning techniques to predict suspicious and non-suspicious transactions automatically using Bayesian network classifiers, such as K2, Tree Augmented Naïve Bayes (TAN), and Naïve Bayes, logistic, and J48 classifiers. All classifiers achieved accuracy higher than 95% compared with the results obtained before preprocessing the dataset. These results are similar to those reported in this study, but it presents worse results when it comes to assessing legitimate transactions.

Awoyemi et al. (2017) analyzed the performance of Naive Bayes, KNN, and logistic regression on financial fraud data by developing a hybrid technique of under sampling and oversampling the asymmetric data (similar to the methodology described in the present study). All three techniques were applied to the raw and pre-processed data, with results showing optimal accuracies for Naive Bayes, KNN, and logistic regression of 97.92%, 97.69%, and 54.86%, respectively. Likewise, similar studies (Mytnyk et al., 2023) indicate that the logistic regression algorithm obtained the best results, with an AUC value of approximately 94.60%.

There is also other research in which the results obtained are significantly lower than those obtained in this study. In this way, authors such as Detthamrong et al. (2024) present an efficiency of 0.9286 in the algorithm with the best results (in this case through Logistic Regression. Recent works such as the one presented by Professor Rao Moparthi present lower results (precision of 88.32%) when combining legitimate with non-legitimate operations (Moparthi, 2024). The advantages of the model developed in this paper over some of the existing literature lie in the high accuracy efficiency in handling unbalanced data sets, which is a common challenge in fraud detection (Alshameri & Xia, 2023). This is the reason for choosing the Random Forest supervised learning algorithm for the present work as it allows us to capture complex patterns in the data, which is crucial for detecting anomalies in highly unbalanced datasets. On the other hand, the results obtained are highly satisfactory and present, to a large extent, a novelty with respect to the rest of the existing academic work, since it is necessary to analyze them not only with respect to the percentage of success in fraudulent operations (95.79%), but also considering the success rate in legitimate operations (100%). It is precisely this point regarding false negatives that represents an advance in the methodology used, as it allows highly robust results in both aspects. In other studies, and with other learning algorithms, interesting results are obtained when assessing non-legitimate operations, but this loses validity as it is not as reliable with legitimate operations.

It is important to recognize that our study presents certain limitations that should be considered when interpreting the results. First, the data used comes only from a single financial institution, which suggests that the results obtained may not be fully generalizable to a broader context that includes the operations of several financial institutions. This limitation could lead to differences in results when applied to datasets containing transactions from multiple financial institutions. Second, although the sample size used in our dataset is considerably large, it is important to note that it does not represent the totality

of banking transactions. This suggests that there is a possibility that certain trends or patterns present in the full dataset may not be fully reflected in our sample, which could influence the accuracy and generalizability of our model. In addition, it is critical to recognize that the data come from a banking institution located in a developed country. Therefore, there is a possibility that the specific characteristics of bank transfers in this environment may not be fully transferable to developing or underdeveloped areas. Differences in banking practices, regulations, and financial behaviors across regions may influence the ability of our model to generalize its results outside the context for which it was trained. Therefore, although our study offers valuable insights into the detection of fraudulent wire transfers, it is important to keep these limitations in mind when interpreting and applying the results to different banking contexts or environments.

Despite these limitations, as already indicated in this paper, academic research on fraud detection linked to the financial sphere is becoming necessary for all types of organizations and, more importantly, for financial institutions. Therefore, although the work refers to a specific case of fraud -banking transactions- and to a specific financial institution, the methodology used allows its application to be extrapolated in a relatively simple way to any similar reality. In other words, one of the advantages of the work is its scalability, since similar studies could be carried out using databases from any other financial institution. It should be noted that the types and patterns of fraud in banking transactions vary by country due to factors such as financial regulation, the level of banking digitalization and cybersecurity infrastructure. Thus, in the European Union, the PSD2 directive obliges banks to implement strong authentication to reduce fraud; in countries such as the United States, although there are variations according to the laws of each state, consumer protections may be laxer compared to Europe; while in Latin America (for example), regulation is more uneven with some countries implementing strong security measures and others with more vulnerable systems (Mozdzynski, 2017). However, the methodology proposed in this paper is extrapolable to any type of operation even with different regulatory standards since it refers to the study of the own internal data available to the various financial institutions. In other words, the different regulations may limit the number and volume of fraudulent operations but, ultimately, it is up to the institution itself to use the necessary tools to limit the impact of these fraudulent operations.

Finally, in addition to financial institutions, governments play an important role in the fight against online fraud. It is crucial that they develop information and awareness campaigns about online banking fraud, especially targeting vulnerable groups such as the elderly, who may be less tech-savvy and, therefore, more susceptible to falling into cyber traps (Albert et al., 2024; Náñez Alonso et al., 2024). By sharing responsibilities between financial institutions and governments, the security of the financial system as a whole can be significantly strengthened. Taking proactive measures and educating the public about online threats are key steps in protecting financial assets (Kaczmarek et al., 2021); and ensuring the stability of the banking system in an ever-changing digital environment. Although this study focuses on bank transfers, the developed models demonstrate significant potential for adaptation to other sectors where fraudulent transactions pose critical challenges. The textile industry, particularly within the context of sustainability and the circular economy, is one such area. Fraudulent operations in this domain can take various forms, including payments for products falsely labeled as sustainable or recycled, misrepresentation of certifications or standards, and the diversion of funds intended for recycling initiatives. These fraudulent practices not only undermine consumer trust but also compromise the integrity of global efforts toward environmental sustainability. Applying algorithms such as Random Forest or neural networks in the textile sector could enhance the detection of anomalies within financial and transactional data, making it possible to identify patterns of irregularities early on. For example, such models could be used to monitor payment flows in donation-based recycling programs, verifying the legitimacy of transactions and ensuring that resources are allocated correctly. Similarly, these techniques could help uncover inconsistencies in supply chains, such as discrepancies between reported and actual recycled material usage, thereby preventing the commercialization of falsely labeled products. By extending the capabilities of these machine learning models to the textile industry, it becomes possible to strengthen transparency, protect stakeholders from financial misconduct, and promote trust in sustainable practices. This demonstrates how the insights gained from addressing bank transfer fraud can provide a foundation for tackling broader challenges in sectors with similar vulnerabilities to transactional fraud.

Conclusions

Fraud is a pressing problem in banking environments that has been spreading and becoming more sophisticated with the development of the internet and digital technologies. Every day, thousands of transfers are issued from any bank, which is impossible for a human to supervise, let alone in real-time. Artificial intelligence, in its machine-learning branch, can be a powerful ally for this task. The task of separating legitimate from fraudulent transfers falls into a group of binary classification problems with supervised algorithms in machine learning. These algorithms analyze information from thousands of observations, detecting patterns - often imperceptible to the human eye - that can lead to a fraud case being considered and that can be used to generate a predictive model. In this research, machine learning models based on the following algorithms were evaluated: K Nearest neighbors, naive Bayes, support vector machines, random forest, and neural networks. In view of the results, it can be concluded that the best candidate is Random, which, after having been tested with data from 141,174 transfers, of which 141,079 were legitimate and 95 fraudulent, has successfully identified 100% of the former, being wrong only in four cases of fraud that it was unable to detect, i.e. 95.79% of fraud cases detected. These are commendable results, especially when the input data are heavily unbalanced.

The results reinforce the relevance of exploring machine learning approaches in the fight against financial fraud. It highlights the need for further research on complementary techniques such as the use of blockchain, tools to improve the generalization of models and strategies to adapt them to different cultural and regulatory contexts. It is also recommended to continue working on the calibration and periodic updating of models to adapt to new tactics used by cybercriminals. These findings have important implications for banking professionals. The implementation of models such as Random Forest can significantly improve transactional security, enabling more efficient and accurate real-time detection, reducing reliance on manual processes and minimizing false positives. In addition, the research underscores the importance of addressing data imbalance, a common challenge in this area, through advanced preprocessing techniques and model optimization. As indicated in the previous points, the proposed model can be applied to all financial institutions and is applicable in different regulatory environments. Similarly, work is being carried out on extensions to this article -following the methodology used- for use in the analysis of fraudulent transactions involving credit cards. However, its application can also be applied to a large number of operations in which financial fraud can occur, such as mobile banking applications, electronic transactions, payment methods, payment service operators, etc. Although this research has focused on the banking sector, its implications can be extended to other sectors vulnerable to transactional fraud, such as the e-commerce and logistics industries, promoting advances in the transparency, reliability and sustainability of financial and commercial activities.

Author contributions

CRediT: **Pedro María Preciado Martínez**: Formal analysis, Investigation, Resources, Software; **Ricardo Francisco Reier Forradellas**: Conceptualization, Formal analysis, Investigation, Methodology, Project administration, Visualization, Writing – original draft; **Luis Miguel Garay Gallastegui**: Methodology, Supervision, Validation, Visualization, Writing – review & editing; **Sergio Luis Náñez Alonso:** Conceptualization, Investigation, Methodology, Project Administration, Writing – Original Draft, Writing – Proofreading and Editing. All authors have approved the final manuscript.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This research was supported by the EUROPEAN COMMISSION-Horizon Europe Framework Program under Grant 101159060AIdesignTEX.

About the authors

Pedro María Preciado Martínez is a senior project manager and software engineer in the Technology and Innovation Unit at Caja Almendralejo. He holds a master's degree in Artificial Intelligence from Universidad Católica de Ávila and a degree in Computer Engineering from Universidad de Extremadura. His expertise lies in the architecture, analysis, and development of banking services, financial applications, payment systems, mobile banking, and digital solutions such as document management, web services, and digital signature systems. Pedro has been actively contributing to the technological advancements at Caja Almendralejo for over 19 years, managing projects and leading software engineering initiatives to improve the institution's service offerings.

Ricardo Reier Forradellas is Associate Professor and Director of the Ávila Business School at the Catholic University of Ávila (UCAV). With more than twelve years of experience, he directs multiple master's programs in areas such as MBA, Artificial Intelligence and Digital Transformation. He is also Director of the UCAV-CEOE Ávila Chair. Prior to his academic career, he worked as Head of Finance at Banco Santander Consumer Finance. He holds a PhD Cum Laude from UCAV and an MBA from Universidad Pontificia Comillas ICAI-ICADE.

Luis Miguel Garay Gallastegui is Director of Computer Science and Technology at the International University of La Rioja (UNIR) since April 2023. Researcher in the DEKIS group and professor in areas such as Digital Marketing, Data Science and Artificial Intelligence since 1998, he has also worked at Telefónica for more than 25 years in digital transformation roles. He holds a PhD in Artificial Intelligence from the University of Deusto and a management development program from IE Business School. He publishes on topics of digital communication and innovative business models.

Sergio Luis Nañez Alonso is Associate Professor and Coordinator of the Avila Business School at the Catholic University of Avila (UCAV). PhD. in Economics and Law from CEU-San Pablo University, with Cum Laude, he also holds a degree in Law and Business Administration. He has worked at the UCAV since 2011, teaching Law and Economics subjects, and is recognized for his outstanding teaching work and participation in international congresses. His research focuses on taxation, economic policy, and cryptocurrencies. In addition, he has led European projects on entrepreneurship and conducted international academic stays.

ORCID

Ricardo Francisco Reier Forradellas http://orcid.org/0000-0002-4790-0351
Luis Miguel Garay Gallastegui http://orcid.org/0000-0002-2119-4532
Sergio Luis Náñez Alonso http://orcid.org/0000-0001-5353-2017

Data availability statement

The data supporting the findings of this study are available from the corresponding author, Sergio Luis Náñez Alonso (sergio.nanez@ucavila.es), upon reasonable request.

References

Abdul Rani, M. I., Syed Mustapha Nazri, S. N. F., & Zolkaflil, S. (2024). A systematic literature review of money mule: Its roles, recruitment and awareness. *Journal of Financial Crime*, *31*(2), 347–361. https://doi.org/10.1108/JFC-10-2022-0243

Afriyie, J. K., Tawiah, K., Pels, W. A., Addai-Henne, S., Dwamena, H. A., Owiredu, E. O., Ayeh, S. A., & Eshun, J. (2023). A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. *Decision Analytics Journal*, *6*, 100163. https://doi.org/10.1016/j.dajour.2023.100163

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020). Analysis of cyber-crime effects on the banking sector using the balanced score card: A survey of literature. *Journal of Financial Crime*, *27*(3), 945–958. https://doi.org/10.1108/JFC-03-2020-0037

Albert, J. F., Gómez Fernández, N., & Náñez Alonso, S. L. (2024). Monedas sociales en la era digital: Retos y oportunidades. *CIRIEC-España, Revista de Economía Pública, Social y Cooperativa*, *110*(110), 163–200. https://doi.org/10.7203/CIRIEC-E.110.25755

Alfaiz, N. S., & Fati, S. M. (2022). Enhanced credit card fraud detection model using machine learning. *Electronics*, *11*(4), 662. https://doi.org/10.3390/electronics11040662

Al-Hashedi, K. G., & Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. *Computer Science Review*, *40*, 100402. https://doi.org/10.1016/j.cosrev.2021.100402

Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial fraud detection based on machine learning: A systematic literature review. *Applied Sciences*, *12*(19), 9637. https://doi.org/10.3390/app12199637

Alshameri, F., & Xia, R. (2023). Credit card fraud detection: An evaluation of SMOTE resampling and machine learning model performance. *International Journal of Business Intelligence and Data Mining*, *23*(1), 1–13. https://doi.org/10.1504/IJBIDM.2023.131791

Al-Surkhi, W., & Maqableh, M. (2024). The impact of cybercrime on internet banking adoption. In M. A. Al-Sharafi, M. Al-Emran, G. W. H. Tan, & K. B. Ooi (Eds.), *Studies in computational intelligence* (pp. 231–245). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-61463-7_12

Amasiatu, C. V., & Shah, M. H. (2018). First party fraud management: Framework for the retail industry. *International Journal of Retail & Distribution Management*, *46*(4), 350–363. https://doi.org/10.1108/IJRDM-10-2016-0185

Analytics Vidhya. (2016). *Imbalanced classification problems in R*. https://www.analyticsvidhya.com/blog/2016/03/practical-guide-deal-imbalanced-classification-problems/

Arfeen, A. A., & Khan, B. M. A. (2023). Empirical analysis of machine learning algorithms on detection of fraudulent electronic fund transfer transactions. *IETE Journal of Research*, *69*(11), 7920–7932. https://doi.org/10.1080/03772063.2022.2048700

Arner, D. W., Barberis, J., & y Buckley, R. P. (2016). The evolution of Fintech: A new post-crisis paradigm. *Georgetown Journal of International Law*, *47*(4), 1271–1319.

Awoyemi, J.O., Adetunmbi, A.O., Oluwadare, S.A. (2017, October 29-31). Credit card fraud detection using machine learning techniques: A comparative analysis. In *International Conference on Computing Networking and Informatics (ICCNI)*, Lagos. Scientific Research Publishing Inc.

Azhar, S., Shahi, M., & Chhapola, V. (2020). E-Banking frauds. In *Encyclopedia of criminal activities and the deep web* (pp. 905–918). IGI Global. https://doi.org/10.4018/978-1-5225-9715-5.ch061

Bello, H. O., Idemudia, C., & Iyelolu, T. V. (2024). Integrating Machine Learning and Blockchain: Conceptual frameworks for real-time fraud detection and prevention. *World Journal of Advanced Research and Reviews*, *23*(1), 056–068.

Bolton, R. y., & Hand, D. (2002). Statistical fraud detection: A review. *Statistical Science*, *17*(3), 235–255. https://doi.org/10.1214/ss/1042727940

Borketey, B. (2024). Real-time fraud detection using machine learning. *Journal of Data Analysis and Information Processing*, *12*(02), 189–209. https://doi.org/10.4236/jdaip.2024.122011

Campus, K. (2018). Credit card fraud detection using machine learning models and collating machine learning models. *International Journal of Pure and Applied Mathematics*, *118*(20), 825–838.

Carbo-Valverde, S., Cuadros-Solas, P., & Rodríguez-Fernández, F. (2020). A machine learning approach to the digitalization of bank customers: Evidence from random and causal forests. *PloS One*, *15*(10), e0240362. https://doi.org/10.1371/journal.pone.0240362

Chauhan, V. K., Dahiya, K., & Sharma, A. (2019). Problem formulations and solvers in linear SVM: A review. *Artificial Intelligence Review*, *52*(2), 803–855. https://doi.org/10.1007/s10462-018-9614-6

Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: Synthetic minority over-sampling technique. *Journal of Artificial Intelligence Research*, *16*, 321–357. https://doi.org/10.1613/jair.953

Chen, S., Webb, G. I., Liu, L., & Ma, X. (2020). A novel selective naïve Bayes algorithm. *Knowledge-Based Systems*, *192*, 105361. https://doi.org/10.1016/j.knosys.2019.105361

Cherif, A., Badhib, A., Ammar, H., Alshehri, S., Kalkatawi, M., & Imine, A. (2023). Credit card fraud detection in the era of disruptive technologies: A systematic review. *Journal of King Saud University - Computer and Information Sciences*, *35*(1), 145–174. https://doi.org/10.1016/j.jksuci.2022.11.008

Chicco, D., Tötsch, N., & Jurman, G. (2021). The Matthews correlation coefficient (MCC) is more reliable than balanced accuracy, bookmaker informedness, and markedness in two-class confusion matrix evaluation. *BioData Mining*, *14*(1), 13. https://doi.org/10.1186/s13040-021-00244-z

Coyle, D. (2016). *Making the most of platforms: A policy research agenda*. Toulouse School of Economics - JeanJacques Laffont Digital Chair Working Paper.

Cuadros-Solas, P. J. (2019). Hacia una nueva tecnología bancaria. Aplicaciones e impacto en la banca comercial. *Papeles de Economía Española*, *162*, 126–140.

Cui, J., Yan, C., & Cheng, W. (2021). A credible individual behavior profiling method for online payment fraud detection. In Proceedings of the 2021 4th International Conference on Data Storage and Data Engineering. ACM. https://doi.org/10.1145/3456146.3456151

Dávila-Morán, R. C., Castillo-Sáenz, R. A., Vargas-Murillo, A. R., Velarde Dávila, L., García-Huamantumba, E., García-Huamantumba, C. F., Pasquel Cajas, R. F., & Guanilo Paredes, C. E. (2023). Application of machine learning models in fraud detection in financial transactions. *Data and Metadata*, *2*, 109. https://doi.org/10.56294/dm2023109

Detthamrong, U., Chansanam, W., Boongoen, T., & Iam-On, N. (2024). Enhancing fraud detection in banking using advanced machine learning techniques. *International Journal of Economics and Financial Issues*, *14*(5), 177–184. https://doi.org/10.32479/ijefi.16613

Dhankhad, S., Mohammed, E., & Far, B. (2018, July). Supervised machine learning algorithms for credit card fraudulent transaction detection: A comparative study. In *2018 IEEE International Conference on Information Reuse and Integration (IRI)* (pp. 122–125). IEEE.

Dong, C., Jin, X., Gao, W., Wang, Y., Zhang, H., Wu, X., Yang, J., & Liu, X. (2021, April 27). *One backward from ten forward, subsampling for large-scale deep learning*. arXiv:2104.13114 https://arxiv.org/abs/2104.13114

European Banking Authority. (2021). *Report on the use of digital platforms (Issue September)*.

Ferrari, R. (2016). FinTech impact on retail banking: from a universal banking model to banking verticalization. In S. Chishti & J. Barberis (Eds.), *The FinTech book: The financial technology handbook for investors, entrepreneurs and visionaries* (pp. 248–252). Wiley.

Garay Gallastegui, L. M., Reier Forradellas, R., & Náñez Alonso, S. L. (2024). Applying advanced sentiment analysis for strategic marketing insights: A case study of BBVA using machine learning techniques. *Innovative Marketing*, *20*(2), 100–115. https://doi.org/10.21511/im.20(2).2024.09

González-Páramo, J. M. (2017). Financial innovation in the digital age: Challenges for regulation and supervision. *Revista de Estabilidad Financiera*, *32*, 9–37.

Gupta, J. (2023). Credit card fraud detection using machine learning algorithms. *International Journal of Science and Research (IJSR)*, *12*(11), 1774–1779. https://doi.org/10.21275/SR231123121203

Hans, S. (2016). *Why artificial intelligence is a game changer for risk management (Deloitte Development LLC, Ed.)*. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-ai-risk-powers-performance.pdf

Ileberi, E., Sun, Y., & Wang, Z. (2022). A machine learning based credit card fraud detection using the GA algorithm for feature selection. *Journal of Big Data*, *9*(1), 24. https://doi.org/10.1186/s40537-022-00573-8

Jain, R. B., & Puri, M. (2020). An approach towards the development of scalable data masking for preserving privacy of sensitive business data. In *Advances in Intelligent Systems and Computing* (pp. 733–743). Springer Singapore. https://doi.org/10.1007/978-981-15-0199-9_63

Jiao, L., & Li, H. (2023). *Research on financial fraud identification model based on privacy-preserving machine learning* [Paper presentation]. 2023 4th International Conference on Machine Learning and Computer Application. https://doi.org/10.1145/3650215.3650326

Jubraj, R., Graham, T., & Ryan, E. (2018). Redefine banking with artificial intelligence. In Accenture (Ed.), *The intelligent bank* (p. 9). Accenture. https://www.accenture.com/_acnmedia/pdf-68/accenture-redefine-banking.pdf

Kaczmarek, J., Alonso, S. L. N., Sokołowski, A., Fijorek, K., & Denkowska, S. (2021). Financial threat profiles of industrial enterprises in Poland. *Oeconomia Copernicana*, *12*(2), 463–498. https://doi.org/10.24136/oc.2021.016

Kemp, S., Miró-Llinares, F., & Moneva, A. (2020). The dark figure and the cyber fraud rise in Europe: Evidence from Spain. *European Journal on Criminal Policy and Research*, *26*(3), 293–312. https://doi.org/10.1007/s10610-020-09439-2

Krishna, K. G., Kulkarni, P., & Natraj, N. A. (2023). *Use of big data technologies for credit card fraud prediction* [Paper presentation]. International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), pp. 1408–1413.

Kubat, M., & Matwin, S. (1997). *Addressing the curse of imbalanced training sets: One-sided selection*. https://sci2s.ugr.es/keel/pdf/algorithm/congreso/kubat97addressing.pdf

Liu, C., Chan, Y., Hasnain, S., & Fu, H. (2015). Financial fraud detection model: Based on random forest. *International Journal of Economics and Finance*, *7*(7), 1–3. https://doi.org/10.5539/ijef.v7n7p178

Liu, S., Lin, G., Han, Q.-L., Wen, S., Zhang, J., & Xiang, Y. (2019). DeepBalance: Deep-Learning and fuzzy oversampling for vulnerability detection. *IEEE Transactions on Fuzzy Systems*, 1–1. https://doi.org/10.1109/TFUZZ.2019.2958558

Liu, Y., Yu, F. R., Li, X., Ji, H., & Leung, V. C. M. (2020). Blockchain and machine learning for communications and networking systems. *IEEE Communications Surveys & Tutorials*, *22*(2), 1392–1431. https://doi.org/10.1109/COMST.2020.2975911

Mangala, D., & Soni, L. (2023). A systematic literature review on frauds in banking sector. *Journal of Financial Crime*, *30*(1), 285–301. https://doi.org/10.1108/JFC-12-2021-0263

Manikandaprabhu, P., Prasanna, S., Sivaranjan, K., & Senthilkumar, R. (2023). Fraudulent banking transaction classification using deeplearning algorithm. *International Journal of Advanced Research in Science, Communication and Technology*, *3*(1), 68–74. https://doi.org/10.32479/ijefi.16613

Mehdiabadi, A., Tabatabeinasab, M., Spulbar, C., Karbassi Yazdi, A., & Birau, R. (2020). Are we ready for the challenge of banks 4.0? Designing a roadmap for banking systems in industry 4.0. *International Journal of Financial Studies*, *8*(2), 32. https://doi.org/10.3390/ijfs8020032

Minastireanu, E. A., & Mesnita, G. (2019). An analysis of the most used machine learning algorithms for online fraud detection. *Informatica Economica*, *23*(1), 5–16. https://doi.org/10.12948/issn14531305/23.1.2019.01

Moparthi, N. R. (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

Mozdzynski, D. (2017). The conceptions of new payment method base on revised payment services directive (PSD2). *Information Systems in Management*, *6*(1), 50–60. https://doi.org/10.22630/ISIM.2017.6.1.5

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

Náñez Alonso, S. L., Jorge-Vazquez, J., Arias, L. G., & del Nogal, N. M. (2024). What factors are limiting financial inclusion and development in Peru? Empirical evidence. *Economies*, *12*(4), 93. https://doi.org/10.3390/economies12040093

Odukoya, O. O., & Samsudin, R. S. (2021). Knowledge capability and fraud risk assessment in Nigeria deposit money banks: The mediating effect of problem representation. *Cogent Business & Management*, *8*(1), 2–5. https://doi.org/10.1080/23311975.2021.1899450

Ozili, P. K., & Alonso, S. L. N. (2024). Central bank digital currency adoption challenges, solutions, and a sentiment analysis. *Journal of Central Banking Theory and Practice*, *13*(1), 133–165. https://doi.org/10.2478/jcbtp-2024-0007

Pal, M. (2005). Random forest classifier for remote sensing classification. *International Journal of Remote Sensing*, *26*(1), 217–222. https://doi.org/10.1080/01431160412331269698

Papernot, N., & McDaniel, P. (2018). Deep k-nearest neighbors: Towards confident, interpretable and robust deep learning. arXiv:1803.0476. https://doi.org/10.48550/arXiv.1803.04765

Paraná, E. (2024). Artificial intelligence and the digitalization of finance in Latin America: Evidence from Brazil. *Globalizations*, 1–20. https://doi.org/10.1080/14747731.2024.2415257

Phiri, J., Lavhengwa, T., & Segooa, M. A. (2024). Online banking fraud detection: A comparative study of cases from South Africa and Spain. *South African Journal of Information Management*, *26*(1), 1–8. https://doi.org/10.4102/sajim.v26i1.1763

Phua, C., Lee, V., Smith, K., & Gayler, R. (2005). A comprehensive survey of data mining-based fraud detection research. arXiv:1009.6119. https://arxiv.org/ftp/arxiv/papers/1009/1009.6119.pdf

Poudel, S., Movinuddin, Gutta, S., Kommu, R. K., Upadhyay, J., Hasan, M. N., & Poudel, K. (2024). Credit card batch processing in banking system. In *Proceedings of the Second International Conference on Advances in Computing Research (ACR'24)* (pp. 83–96). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-56950-0_8

Purdy, M., & Daugherty, P. (2016). *Why artificial intelligence is the future of growth*. Accenture. https://dl.icdst.org/pdfs/files2/2aea5d87070f0116f8aaa9f545530e47.pdf

Qawqzeh, Y., & Ashraf, M. (2023). A fraud detection system using decision trees classification in an online transactions. In Proceedings of the 2023 12th International Conference on Software and Computer Applications. ACM. https://doi.org/10.1145/3587828.3587860

Rahman, M., Ming, T. H., Baigh, T. A., & Sarker, M. (2023). Adoption of artificial intelligence in banking services: An empirical analysis. *International Journal of Emerging Markets*, *18*(10), 4270–4300. https://doi.org/10.1108/IJOEM-06-2020-0724

Ramos, S., Perez-Lopez, J. A., Abreu, R., & Nunes, S. (2024). Impact of fraud in Europe: Causes and effects. *Heliyon*, *10*(22), e40049. https://doi.org/10.1016/j.heliyon.2024.e40049

Reier Forradellas, R. F., Náñez Alonso, S. L., Jorge-Vazquez, J., & Rodriguez, M. L. (2020). Applied machine learning in social sciences: Neural networks and crime prediction. *Social Sciences*, *10*(1), 4. https://doi.org/10.3390/socsci10010004

Sailusha, R., Gnaneswar, V., Ramesh, R., & Rao, G. R. (2020). *Credit card fraud detection using machine learning* [Paper presentation]. 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 1264–1270). IEEE. https://doi.org/10.1109/ICICCS48265.2020.9121114

Santamaría Ruíz, W. (2010). *Modelo de detección de fraude basado en el descubrimiento simbólico de reglas de clasificación extraídas de una red neuronal* [Tesis de Maestría]. Universidad Nacional de Colombia]. https://repositorio.unal.edu.co/handle/unal/6851

Sawdatkar, P., Singh, D., & Kundu, K. (2023). Applications of machine learning in the manufacturing sector. In R. Kumar, S. Rani, & S. S. Khangura (Eds.), *Machine learning for sustainable manufacturing in industry 4.0* (pp. 201–231). CRC Press. https://doi.org/10.1201/9781003453567-11

Sharma, N. V., & Yadav, N. S. (2021). An optimal intrusion detection system using recursive feature elimination and ensemble of classifiers. *Microprocessors and Microsystems*, *85*, 104293. https://doi.org/10.1016/j.micpro.2021.104293

Sharma, N., & Sharma, D. (2018). Rising toll of frauds in banking: A threat for the Indian economy. *Journal of Technology Management for Growing Economies*, *9*(1), 71–88. https://doi.org/10.15415/jtmge.2018.91003

Sohony, I., Pratap, R., & Nambiar, U. (2018). *Ensemble learning for credit card fraud detection. Proceedings* [Paper presentation]. Of the ACM India Joint International Conference on Data Science and Management of Data, pp. 289–294. https://doi.org/10.1145/3152494.3156815

Stiglitz, J. (2017). *The revolution of information economics: The past and the future*. NBER Working Papers 23780. National Bureau of Economic Research. https://doi.org/10.3386/w23780

Tambe Ebot, A. (2023). Advance fee fraud scammers' criminal expertise and deceptive strategies: A qualitative case study. *Information & Computer Security*, *31*(4), 478–503. https://doi.org/10.1108/ICS-01-2022-0007

Toloba, C., & Del Río, J. M. (2020). La perspectiva de la digitalización de la banca española: Riesgos y oportunidades. *Revista de Estabilidad Financiera*, *97*(Spring 2020), 79–98.

Vergara, D., Del Bosque, A., Lampropoulos, G., & Fernández-Arias, P. (2025). Trends and applications of artificial intelligence in project management. *Electronics*, *14*(4), 800. https://doi.org/10.3390/electronics14040800

Vergara, D., Lampropoulos, G., Antón-Sancho, Á., & Fernández-Arias, P. (2024). Impact of artificial intelligence on learning management systems: A bibliometric review. *Multimodal Technologies and Interaction*, *8*(9), 75.https://doi.org/10.3390/mti8090075

Wang, Y., Zhang, Y., Lu, Y., & Yu, X. (2020). A comparative assessment of credit risk model based on machine learning. *Procedia Computer Science*, *174*, 143. https://doi.org/10.1016/j.procs.2020.06.069

Wickramanayake, B., Geeganage, D. K., Ouyang, C., & Xu, Y. (2020). A survey of online card payment fraud detection using data mining-based methods. arXiv:2011.14024. https://doi.org/10.48550/arXiv.2011.14024

Yee, O. S., Sagadevan, S., & Malim, N. H. A. H. (2018). Credit card fraud detection using machine learning as data mining technique. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, *10*(1–4), 23–27.

Zieni, R., Massari, L., & Calzarossa, M. C. (2023). Phishing or not phishing? A survey on the detection of phishing websites. *IEEE Access*, *11*, 18499–18519. https://doi.org/10.1109/ACCESS.2023.3247135

Appendix

Table A1. Original dataset fields with transfers.

Field	Description
sent	Internal data of the entity
Operator	Operator who initiates the transfer. There are certain special operators reserved for services: cashier, electronic banking, immediate transfers, etc.
process	Internal data of the entity
sw_accounting	Accounting switch (Internal data of the entity)
Identifier	Identifier of the channel through which the transfer was ordered (via counter, virtual banking, in cash, by support, etc.)
external_ref	External reference number
num_transfer	Transfer number
TransferDate	Transfer date, in YYYYMMDD format
value_date	Value date of the transfer, in YYYYMMDD format
PaymentType	Type of payment. Can be SEPA (conventional transfer) or INST (immediate transfer)
TransferType	Internal data of the entity
DestinationBIC	BIC code of the beneficiary's account
OriginBranch	Branch number of the transfer origin
ref_beneficiary	Blank
ref_ordering	Blank
expense_clause	Internal data of the entity (Expense Clause)
AmountEuros	Amount of the transfer
commission_euro	Commission applied (data hidden)
OrderingCode	Identifying code of the ordering party (DNI, CIF, NIE, etc.)
OrderingCity	Town of the ordering client
OrderingProvince	Province of the ordering client
OrderingIBAN	IBAN of the ordering client
BeneficiaryName	Name of the beneficiary client
BeneficiaryAddress	Address of the beneficiary client
BeneficiaryCity	Town of the beneficiary client
BeneficiaryProvince	Province of the beneficiary client
BeneficiaryCountry	Country of the beneficiary client
BeneficiaryIBAN	IBAN of the beneficiary client
concept1	First transfer concept
concept2	Second transfer concept
type_concept	Internal data of the entity (Type of Concept)
filler15	Internal data of the entity (Filler Data)
entity	Working entity
PurposeCategory	Identifier of the purpose of the transfer
int_local	Internal data of the entity (Local Interest)
name_for_account	Blank
sem_additional	Internal data of the entity (Additional Semantic)
sw_reconcile1	Internal data of the entity (Switch for Reconciliation 1)
sw_reconcile2	Internal data of the entity (Switch for Reconciliation 2)
Fraud	Indicator of whether the transfer is legitimate (0) or fraudulent (1). This will be the target or goal that the model must predict.
sent	Internal data of the entity
Operator	Operator who initiates the transfer. There are certain special operators reserved for services: cashier, electronic banking, immediate transfers, etc.
process	Internal data of the entity
sw_accounting	Accounting switch (Internal data of the entity)

Source: Own elaboration based on dataset.

Table A2. Eliminated fields.

Field	Description
sent	Internal data of the entity
process	Internal data of the entity
sw_accounting	Internal data of the entity
external_ref	Reference number, which does not add value to the analysis
num_transfer	Transfer number, which does not add value to the analysis
value_date	Data calculated internally from the transfer date
bic_origin	Always the same value
ref_beneficiary	Blank
ref_ordering	Blank
expense_clause	Internal data of the entity
commission_euro	Always zero
name_ordering	The ordering code (DNI, CIF, NIE, etc.) provides the same information, thus it is redundant
address_ordering	The ordering code (DNI, CIF, NIE, etc.) provides the same information, thus it is redundant
country_ordering	Always the same value
concept1	Blank
concept2	Blank
type_concept	Internal data of the entity
filler15	Internal data of the entity
entity	Always the same value
int_local	Internal data of the entity
name_for_account	Blank
sem_additional	Internal data of the entity
sw_reconcile1	Internal data of the entity
sw_reconcile2	Internal data of the entity

Source: Own elaboration based on dataset.

Table A3. Final columns of the dataset.

Field	Description
Operator	Operator that initiates the transfer. There are certain special operators: ATM (cashier), BANVI (electronic banking), ISCT (immediate transfer service)
Identifier	Identifier of the channel through which the transfer was ordered (via counter, virtual banking, in cash, by support, etc.)
TransferDate	Transfer date, in YYYYMMDD format
PaymentType	Type of payment. Can be SEPA (conventional transfer) or INST (immediate transfer)
TransferType	Internal data of the entity
DestinationBIC	BIC code of the beneficiary's account
OriginBranch	Branch number of the transfer origin
AmountEuros	Amount of the transfer
OrderingCode	Identifying code of the ordering party (DNI, CIF, NIE, etc.)
OrderingCity	Town of the ordering client
OrderingProvince	Province of the ordering client
OrderingIBAN	IBAN of the ordering client
BeneficiaryName	Name of the beneficiary client
BeneficiaryAddress	Address of the beneficiary client
BeneficiaryCity	Town of the beneficiary client
BeneficiaryProvince	Province of the beneficiary client
BeneficiaryCountry	Country of the beneficiary client
BeneficiaryIBAN	IBAN of the beneficiary client
PurposeCategory	Identifier of the purpose of the transfer
NumTxnToday	Number of transfers that the ordering IBAN has issued throughout the day
AvgNumTxn7D	Average daily number of transfers that the ordering IBAN has issued in the previous 7 days
AvgNumTxn7DPrior	Average daily number of transfers that the ordering IBAN has issued in the 7 days prior to the last 7 days
AvgNumTxn30D	Average daily number of transfers that the ordering IBAN has issued in the previous 30 days
AvgNumTxn30DPrior	Average daily number of transfers that the ordering IBAN has issued in the 30 days prior to the last 30 days
AvgNumTxn12M	Average daily number of transfers that the ordering IBAN has issued in the previous 12 months
AvgAmtTxnToday	Average amount of transfers from that day from the ordering IBAN
AvgAmtTxn7D	Average daily amount of transfers that the ordering IBAN has issued in the previous 7 days
AvgAmtTxn7DPrior	Average daily amount of transfers that the ordering IBAN has issued in the 7 days prior to the last 7 days
AvgAmtTxn30D	Average daily amount of transfers that the ordering IBAN has issued in the previous 30 days
AvgAmtTxn30DPrior	Average daily amount of transfers that the ordering IBAN has issued in the 30 days prior to the last 30 days
AvgAmtTxn12M	Average daily amount of transfers that the ordering IBAN has issued in the previous 12 months
NumBnfTxnToday	Number of transfers that the beneficiary IBAN has received on this day (from any ordering party of the entity)
AvgNumBnfTxn7D	Average daily number of transfers that the beneficiary IBAN has received in the previous 7 days (from any ordering party of the entity)
AvgNumBnfTxn30D	Average daily number of transfers that the beneficiary IBAN has received in the previous 30 days (from any ordering party of the entity)
AvgNumBnfTxn12M	Average daily number of transfers that the beneficiary IBAN has received in the last 12 months (from any ordering party of the entity)
AvgAmtBnfTxnToday	Average amount of transfers that the beneficiary IBAN has received on this day (from any ordering party of the entity)
AvgAmtBnfTxn7D	Average amount of transfers that the beneficiary IBAN has received in the previous 7 days (from any ordering party of the entity)
AvgAmtBnfTxn30D	Average amount of transfers that the beneficiary IBAN has received in the previous 30 days (from any ordering party of the entity)
AvgAmtBnfTxn12M	Average amount of transfers that the beneficiary IBAN has received in the last 12 months (from any ordering party of the entity)
Fraud	Indicator of whether the transfer is legitimate (0) or fraudulent (1). This will be the target or goal to be predicted by the model.

Source: Own elaboration based on dataset.