Humanities & Social Sciences Communications

REVIEW ARTICLE

https://doi.org/10.1057/s41599-024-03606-0 OPEN

Financial fraud detection through the application of machine learning techniques: a literature review

Ludivia Hernandez Aros[1✉], Luisa Ximena Bustamante Molano[2], Fernando Gutierrez-Portela[2], John Johver Moreno Hernandez[1] & Mario Samuel Rodríguez Barrero[3]

Financial fraud negatively impacts organizational administrative processes, particularly affecting owners and/or investors seeking to maximize their profits. Addressing this issue, this study presents a literature review on financial fraud detection through machine learning techniques. The PRISMA and Kitchenham methods were applied, and 104 articles published between 2012 and 2023 were examined. These articles were selected based on predefined inclusion and exclusion criteria and were obtained from databases such as Scopus, IEEE Xplore, Taylor & Francis, SAGE, and ScienceDirect. These selected articles, along with the contributions of authors, sources, countries, trends, and datasets used in the experiments, were used to detect financial fraud and its existing types. Machine learning models and metrics were used to assess performance. The analysis indicated a trend toward using real datasets. Notably, credit card fraud detection models are the most widely used for detecting credit card loan fraud. The information obtained by different authors was acquired from the stock exchanges of China, Canada, the United States, Taiwan, and Tehran, among other countries. Furthermore, the usage of synthetic data has been low (less than 7% of the employed datasets). Among the leading contributors to the studies, China, India, Saudi Arabia, and Canada remain prominent, whereas Latin American countries have few related publications.

Introduction

Financial fraud represents a highly significant problem, resulting in grave consequences across business sectors and impacting people's daily lives (Singh et al., 2022). Its occurrence leads to reduced confidence in the economy, resulting in destabilization and direct economic repercussions for stakeholders (Reurink, 2018). Abdallah et al. (2016) define fraud as a criminal act aimed at obtaining money unlawfully. There are diverse types of fraud, such as asset misappropriation, expense reimbursement, and financial statement manipulation. Scholars have classified fraud into three categories: banking, corporate, and insurance (Ali et al., 2022; Nicholls et al., 2021; West and Bhattacharya, 2016).

[1] School of Public Accounting, Universidad Cooperativa de Colombia, 730001 Ibagué-Espinal campus, Ibagué, Colombia. [2] School of Systems Engineering, Universidad Cooperativa de Colombia, 730001 Ibagué-Espinal campus, Ibagué, Colombia. [3] School of Business Administration, Universidad Cooperativa de Colombia, 730001 Ibagué-Espinal campus, Ibagué, Colombia. ✉email: ludivia.hernandez@campusucc.edu.co

The problem becomes evident in the case of financial fraud, evidenced by the 2022 figures of the PricewaterhouseCoopers survey report revealing that 56% of companies globally have fallen victim to some form of fraud. In Latin America, 32% of companies have experienced fraud (PricewaterhouseCoopers, 2022). These alarming statistics align with the findings from Klynveld Peat Marwick Goerdeler (KPMG), indicating that 83% of the surveyed executives reported being targeted by cyberattacks in the past 12 months. Furthermore, 71% had encountered some type of internal or external fraud (KPMG, 2022). These survey results reveal the higher risks of financial fraud faced by companies in Latin America, the United States, and Canada. In this context, traditional approaches, and techniques, as well as manual methods, have lost relevance and effectiveness because they cannot effectively address the complexity and scale of the information involved in detecting financial fraud.

As previously mentioned, despite the interest of organizations in detecting financial fraud using machine learning (ML), current knowledge in this field remains limited. After an initial research phase, specialized literature shows that most researchers have directed their efforts toward the analysis of credit card fraud using a supervised approach (Femila Roseline et al., 2022; Madhurya et al., 2022; Plakandaras et al., 2022; Saragih et al., 2019). In the studies of Ali et al. (2022), Hilal et al. (2022), and Ramírez-Alpízar et al. (2020), ML techniques employing the supervised approach were found to be the most widely used method for detecting financial fraud, compared to the unsupervised, deep learning, reinforcement, and semi-supervised approaches, among others. Moreover, scholars such as Whiting et al. (2012) have compared the performance of data mining models for detecting fraudulent financial statements using data from quarterly and annual financial indexes of public companies from the COMPUSTAT database.

Reurink (2018) has analyzed financial fraud resulting from false financial reports, scams, and misleading financial sales in the context of the financial market. Just like Wadhwa et al. (2020), he presented a wide variety of data mining methods, approaches, and techniques used in fraud detection, in addition to research addressing online banking fraud (Zhou et al., 2018; Moreira et al., 2022; Srokosz et al., 2023) and financial statement fraud (S. Chen, 2016; Ramírez-Alpízar et al., 2020). The abovementioned research works show that the accuracy of ML techniques in developing models for detecting financial fraud has increased (Al-Hashedi and Magalingam, 2021).

The effectiveness of financial fraud detection and prevention depends on the effective selection of appropriate ML techniques to identify new threats and minimize false fraud alarm warnings, responding to the negative impact of financial fraud on organizations (Ahmed et al., 2016). The use of ML techniques has made it possible to identify patterns and anomalies in large financial data sets. However, developments in detection tools, inaccurate classification, detection methods, privacy, computer performance, and disproportionate misclassification costs continue to hinder the accurate and timely detection of financial fraud (Dantas et al., 2022; Mongwe and Malan, 2020; Nicholls et al., 2021; West and Bhattacharya, 2016).

Recently, several studies have reviewed financial statement fraud detection methods in data mining and ML (Gupta and Mehta, 2021; Shahana et al., 2023); however, the present study is different from these past works in the area. These authors established the types of financial fraud and the different data mining techniques and approaches used to detect financial statement fraud. In contrast, our study explains the trends in the use of ML approaches and techniques to detect financial fraud, and it presents the more frequently used datasets in the literature for conducting experiments.

Fraud detection mechanisms using machine learning techniques help detect unusual transactions and prevent cybercrime (Polak et al., 2020). Although each of these approaches uses different methods in their experimentation, a systematic literature review (SLR) shows that the application of each algorithm mirrors performance metrics to determine the accuracy with which it predicts that a financial transaction is fraud. Such metrics include Accuracy, Precision, F1 Score, Recall, and Sensitivity, among others.

The research presented uses a rigorous and well-structured methodology to expand current knowledge on financial fraud detection using machine learning (ML) techniques. Through the use of a systematic literature review that follows adaptations of PRISMA guidelines and Kitchenham's methodology, the study ensures a carefully planned and transparent review process. The sources of information consulted include research articles published in reputable academic databases such as Scopus, IEEE Xplore, Taylor & Francis, SAGE, and ScienceDirect, ensuring that the review covers the most relevant and quality scientific literature in the field of financial fraud and machine learning. Moreover, the study includes a bibliometric analysis using VOSviewer software, which allows identifying trends and patterns within the literature both quantitatively and visually. Based on the 104 articles reviewed, which cover the period 2012–2023, we manage to describe the types of fraud, the models applied, the ML techniques used, the datasets employed, and the metrics of performance reported. These contribute to filling the existing gaps in the literature by providing a comprehensive and up-to-date synthesis of the evidence on the use of machine learning techniques for financial fraud detection, thus laying the groundwork for future research and practical applications in this field.

Our responses to the initial research questions raised are four main contributions that justify this research. Thus, this study contributes to the literature on financial fraud detection by examining the relationship between the current literature on financial fraud detection and ML based on the scholars, articles, countries, journals, and trends in the area. Fraud has been classified as internal and external, with a focus on credit card loan fraud investigations and insurance fraud. The different ML techniques and their models applied to experiments were grouped. The most widely used datasets in financial fraud detection using ML are analyzed according to the 86 articles that contained experiments, highlighting that most of them involve real data. This paper is useful for researchers because it studies and presents the metrics used in supervised and unsupervised learning experiments, providing a clear view of their application in the different models.

Therefore, this study is relevant because it presents in a consolidated and updated manner new contributions derived from experiment results regarding the use of ML, which helps address the problem when financial fraud occurs.

The research work is organized as follows: the section "Methods" comprehensively describes the research method and the questions addressed in the study. Section "Results of the data synthesis" presents the findings encompassing authors, articles, sources, countries, trends, financial fraud types, and datasets with their characteristics to which the detection models using ML techniques were applied, with the results of their metrics. Finally, the section "Discussion and conclusion" highlights the conclusions, including future lines of research in the field.

Methods

The study focuses on SLR, which provides a comprehensive view of the great developments in financial fraud detection. Considering the purpose, scientific guidelines were followed in the

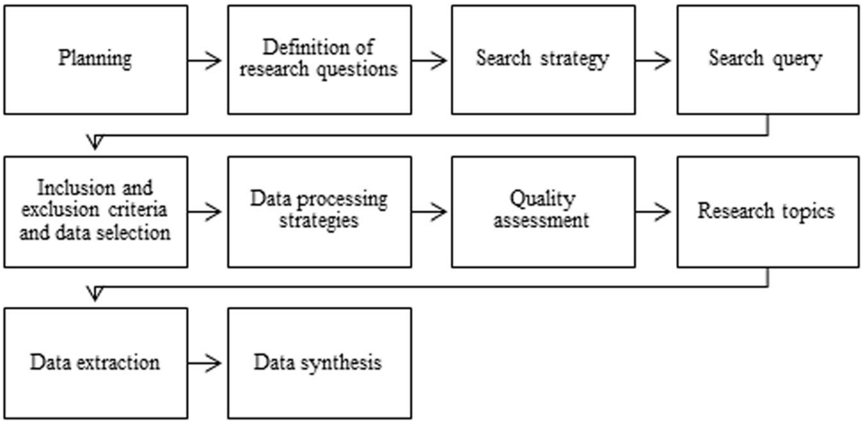

Planning
Definition of research questions
Search strategy
Search query
Inclusion and exclusion criteria and data selection
Data processing strategies
Quality assessment
Research topics
Data extraction
Data synthesis

Fig. 1 Literature review process. Description of the general process used to review the literature in the study area. Authors' own elaboration.

literature review of the PRISMA and Kitchenham methods, which were adapted by the authors (Ashtiani and Raahemi, 2022; Kitchenham and Brereton, 2013; Kitchenham and Stuart, 2007; Kumbure et al., 2022; Moher et al., 2009; Roehrs et al., 2017; Saputra et al., 2023; Wohlin, 2014).

The method used in the SLR was developed with carefully planned and executed activities: (a) planning of the review, (b) definition of research questions, (c) description of the search strategy, (d) consultation concerning the search strategy, (e) selection of the inclusion/exclusion criteria and data selection, (f) description of the quality assessment, (g) investigation of the study topics, (h) description of data extraction, and (i) synthesis of the data.

Each of the activities conducted in this study is explained below.

Planning of the review. The research purpose was established in accordance with the indicated research goals and questions. The analysis focused on research articles published between 2012 and 2023, particularly those using ML methods for financial fraud detection. Accordingly, the SLR procedure presented by Kitchenham and Stuart (2007) and Moher et al. (2009) was implemented following a series of steps adapted and modified by Ashtiani and Raahemi (2022) and Kumbure et al. (2022), as depicted in Fig. 1. Thus, it was possible to ensure a rigorous and objective analysis of the available literature in our field of interest.

The procedures implemented in this review process are discussed in the following subsections.

Definition of research questions. In SLR, research questions are key and decisive for the success of the study (Kitchenham and Stuart, 2007). Therefore, analyzing the existing literature on financial fraud detection through ML techniques and its characteristics, problems, challenges, solutions, and research trends is crucial. Table 1 describes the research questions to provide a structured framework for the study.

Within the proposed systematic review, the questions were fine-tuned, achieving a better classification and thematic analysis. The research questions were categorized into two groups: general questions (GQ) and specific questions (SQ). GQs provide an overview of the current state of the art, that is, a general framework for future research. Meanwhile, SQs focus on specific matters emerging from the application areas of the topic, thereby improving the filtering process of the study.

Description of the search strategy. The search strategy was designed to identify a set of studies addressing the research questions posed. This strategy was to be implemented in two stages. In the first stage, a manual search was conducted by selecting a set of test documents through a defined database. Following the strategy proposed by Wohlin (2014), a snowball search was conducted. This approach involved choosing from a set of initial references (e.g., relevant articles or books addressing the subject matter) and searching for new related references relevant to the study based on these.

In the second stage, an automated search was performed using the technique described by Kitchenham and Brereton (2013), which included preparing a list of the main search terms to be applied in the queries in each database, as indicated in subsection "Search queries".

Manual search. In the study's initial stage, nine journal articles were selected from the test set of papers (Ahmed et al., 2016; Ali et al., 2022; Bakumenko and Elragal, 2022; Gupta and Mehta, 2021; Hilal et al., 2022; Nicholls et al., 2021; Nonnenmacher and Marx Gómez, 2021; Ramírez-Alpízar et al., 2020; West and Bhattacharya, 2016). The manual literature search helped identify articles related to financial fraud detection through ML techniques, which were used as an initial set and were part of the final analysis. In the subsequent stage, a backward and forward snowball search was conducted. This approach involved using the initial set to select the relevant articles.

The backward snowball search process comprised reviewing article titles, including those meeting the inclusion and exclusion criteria. In the forward snowball search, the analysis was performed in the Scopus database to identify studies citing one or more of the articles in the initial set. This filtering method helped identify studies meeting the inclusion and exclusion criteria, eliminate duplicates from the previous set, and analyze articles answering the questions posed, which were retained in the final study set.

Automated search. The research work mainly aimed to obtain a reliable set of relevant studies to minimize bias and increase the validity of the results. To this end, a manual search for articles meeting the inclusion and exclusion criteria was conducted by assessing the abstracts and other sections of articles. We decided to implement an automated search strategy using five databases: Scopus, IEEE Xplore, Taylor & Francis, SAGE, and ScienceDirect, known for their impartiality in the representation of research works, with inclusion and exclusion criteria already defined, thereby complementing the search. Thus, 104 related articles meeting the criteria established in the final set were identified.

Search queries. Studies from 2012 onward were reviewed with keywords such as "financial fraud" and "machine learning" to

Table 1 General and specific research questions.

Identifier	Research question
General questions (GQ)	
GQ1	Which were the most relevant authors, articles, sources, countries, and trends in the literature review on financial fraud detection based on the application of machine learning (ML) models?
GQ2	What types of financial fraud have been identified in ML studies?
GQ3	Which ML models were implemented to detect financial fraud in the datasets?
Specific questions (SQ)	
SQ1	What datasets were used for implementing ML models for financial fraud detection?
SQ2	What were the metrics used to assess the performance of ML models to detect financial fraud?

Table 2 Database search query.

Database	Search query
Scopus	TITLE-ABS-KEY (financial AND fraud AND machine AND learning OR mining AND data OR artificial AND intelligent)
IEEE Xplore	“Financial fraud” AND “machine learning” AND “mining data” OR “artificial intelligent”
Taylor & Francis	[[All: “financial fraud”] AND [All: “machine learning”] AND [All: “mining data”]] OR [All: “artificial intelligent”]
SAGE	“Financial fraud” AND “machine learning” AND “mining data” OR “artificial intelligent”
ScienceDirect	“Financial fraud AND machine learning AND mining data OR artificial intelligent”

identify model-based approaches and associated techniques. Table 2 presents a summary of the queries used in each data source.

Inclusion and exclusion criteria and study selection. The study established inclusion and exclusion criteria, a key process to select the most relevant articles. The exclusion criteria were documents published between 2012 and 2023 (until March), such as conference reviews, book chapters, editorials, and reviews. Further, the availability of the full text of the article was considered. We decided to exclude articles published before 2012 for the following reasons: (i) They were over 11 years old; (ii) Relevant publications prior to 2012 were scarce; and (iii) Sufficient number of articles were available between 2012 and 2023.

For the inclusion and exclusion criteria, appropriate filtering tools were applied to each data source during the search stage. This enabled the automated selection of the most relevant and appropriate studies based on the research goal.

Data processing strategies. In the data processing strategy used, databases were selected following strict inclusion and exclusion criteria to ensure the quality and relevance of the information collected (Table 3). Various databases initially identified the following number of relevant articles: Scopus (28), Taylor & Francis (80), SAGE (71), ScienceDirect (663), and IEEE Xplore (5132). This initial step provides a broad overview of the available literature in the field of financial fraud detection using ML models.

Subsequently, a data removal phase was carried out so as to ensure data integrity, such that the following number of articles (given in parentheses) were removed from each database: Scopus (0), Taylor & Francis (63), SAGE (57), ScienceDirect (636), and IEEE Xplore (5114). This rigorous process ensures the integrity of the data collected and avoids redundancy.

The final step consisted of obtaining the consolidated number of articles included after the selection and exclusion of duplicates: Scopus (28), Taylor & Francis (17), SAGE (14), ScienceDirect (27), and IEEE Xplore (18). This methodological strategy ensured the relevance of the articles that carried out a complete analysis in the field of financial fraud detection using ML models.

Quality assessment. Once the inclusion and exclusion criteria were applied, the remaining articles were assessed for quality. The evaluation criteria used included the purpose of the research; contextualization; literature review; and related works, methods, conclusions, and results. To minimize the empirical obstacles associated with full-text filtering, a set of questions proposed by Roehrs et al. (2017) (see Table 4) was used to validate whether the selected articles met the previously established quality criteria.

Table 3 Inclusion and selection criteria for the search process.

Identifier	Criteria
Inclusion	
I.1	Studies found using the snowball technique and meeting exclusion and quality criteria
I.2	Studies corresponding to the detection of financial fraud through the application of machine learning (ML) techniques
I.3	Studies corresponding to the selected institutional databases
I.4	Studies, including literature review, surveys, and/or experiments
Exclusion	
E.1	Studies not focusing on or not complying with financial fraud anomaly detection.
E.2	Studies not implementing ML techniques
E.3	Type of studies: Conference review, editorial, book chapters, etc.
E.4	Studies with less than five citations
E.5	Studies outside the year range of 2012–2023
E.6	Studies not mentioning data sources
E.7	Articles appearing in different databases

Research topics. In conducting the literature review to understand the current state of published research on the topic, a data orientation process was addressed, including preprocessing techniques and ML models and their metrics. Accordingly, four research topics were defined based on the research goals. They are presented in Table 5.

Data extraction. For data extraction, the necessary attributes were first defined and the information pertaining to the study goals was summarized. Next, the relevant information was identified and obtained through a detailed reading of the full text

Table 4 Set of Questions Posed.

Identifier	Complete text question
SQ.1	Is the purpose of the research clearly and concisely presented in the article?
SQ.2	Does the article provide an adequate review of the literature, background, or context in relation to the research topic?
SQ.3	Is the related work clearly presented in the article and connected with its main contribution?
SQ.4	Does the article sufficiently describe the proposed research architecture or method?
SQ.5	Are the research results clearly and coherently presented in the article?
SQ.6	Is the article's conclusion related to the stated research goals?
SQ.7	Does the article recommend future work, improvements, or additional studies related to the research?

Table 5 Research topics.

Identification	Research topic	Goals
TM.1	Bibliographic information	Identify the annual distribution of the selected articles in the subject of interest Determine the most relevant article and/or journal in the research area Analyze the distribution of the keywords used in the selected articles Identify the most relevant, current studies, and the trend in the area of research based on a systematic literature review
TM.2	Data collection	Analyze the most relevant characteristics and variables of the data sets used in the selected articles
TM.3	Machine learning models	Identify the most used and/or relevant machine learning (ML) models in the area of study and state of the art Identify the techniques implemented with the main ML approaches
TM.4	Assessment and/or performance metrics	Describe the performance metrics commonly used to assess ML models used in financial fraud detection

of each article. The information was then stored in a Microsoft Excel spreadsheet. Data were collected on the attributes specified in Table 6. In Table 6, the "Study" column corresponds to the identifiers of the research topics in Quality Assessment, and the "Subject" column refers to the category to which the different attributes belong. The names of the attributes and a brief description are presented in the last two columns of the table, including additional columns with relevant information.

Data synthesis. Data synthesis included analyzing and summarizing the information observed in the selected articles to address the research questions. To perform this task, a synthesis was conducted following the guidelines proposed by Moher et al. (2009) based on qualitative data. Further, a descriptive analysis was performed to obtain answers to the research questions. Consequently, a qualitative approach to data evidence was followed.

Results of the data synthesis

In this section, the 104 finally selected articles have been considered. The data were synthesized to address the five research questions mentioned.

General questions (GQ)

GQ1: Which were the most relevant authors, articles, sources, countries, and trends in the literature review on financial fraud detection based on the application of machine learning (ML) models?

Authors. The literature on financial fraud detection applying ML models has been studied by a large number of authors. However, some authors stood out in terms of the number of published papers and number of citations. Specifically, the most significant authors with two publications are Ahmed M. (with 318 citations), Ileberi E. (82 citations), Ali A. (20 citations), Chen S. (84 citations), and Domashova J and Kripak E. (each with 6 citations). Other relevant authors with one publication and who have been cited several times are Abdallah A. (with 333 citations), Abbasimehr H. (18 citations), Abd Razak S. (13 citations), Achakzai M. A. K. (5 citations), and Abosaq H. (2 citations). The aforementioned authors have contributed significantly to the development of research in financial fraud detection using ML models (Fig. 2).

Collectively, the researchers have contributed a solid knowledge base and have laid the foundation for future research in financial fraud detection using ML models. Although other researchers contributed to the field, such as Khan, S. and Mishra, B., both with 7 citations, among others, some have been more prominent in terms of the number of papers published. Their collective works have enriched the field and have promoted a greater understanding of the challenges and opportunities in this area.

Articles. As depicted in Fig. 3, clusters 2 (green) and 4 (yellow) present the most relevant research articles on financial fraud detection using ML models. Cluster 2, comprising 9 articles with 357 citations and 32 links, is highlighted because of the significant impact of the articles by Sahin, Huang, and Kim. These articles have the highest number of citations and are deemed to be useful starting points for those intending to dive into this research field. Cluster 4, constituting 6 articles with 158 citations and 27 links, includes the works of Dutta and Kim, who have also been cited considerably.

Articles in clusters 1 (red) and 3 (dark blue) could be valuable sources of information; however, they were observed to have a lower number of citations and links than those in clusters 2 and 4, such as that of Nian K. (62 citations and 4 links) and Olszewski (92 citations and 4 links). However, some articles in these clusters have had a substantial number of citations.

In Cluster 10 (pink), the article by Reurink A. is prominent, with 38 citations. This is followed by the article by Ashtiani M.N. with 10 citations. In Cluster 11 (light green), the article by Hájek P. has 129 citations. In Cluster 12 (grayish blue), the articles by Blaszczynski J. and Elshaar S. have the greatest number of citations, indicating their influence in the field of financial fraud detection.

Table 6 Data extraction attributes.

Study	Subject	Data attributes	Description
TM.1	Bibliographic information	Title	Article title
		Year	Year of publication
		References	Article citation
		Source	Article location
		Purpose	Research goals
		Editors	Article database
		Keywords	Keywords listed in the article
TM.2	Data description	Types of fraud	Selected financial frauds
		Selected variables	Variables of subject interest
		Start period	Data collection start date
		End period	Data collection end date
		Dataset size	Amount of data in the dataset
		Name of the selected dataset	Dataset description
		Dataset type	Specification of normal or anomalous data according to the type of fraud
TM.3	Theoretical concepts and experimental procedure	Origin and author of the dataset	Description of origin and author of the dataset
		Learning approach	Supervised, unsupervised, semi-supervised, deep learning?
		Model (Category)	Model and/or algorithm used
		Model (Subcategory)	Other methods used
		Specifications	Parameters of the final model
		Programming language	Software and/or language used in the study
		Benchmarks	Existing methods used for comparison purposes
		Iterations in the training set	Number of iterations
TM.4	Data preprocessing techniques	Feature selection	Feature selection implementation?
		Feature extraction	Feature extraction implementation?
		Feature construction	Feature construction generation?
		Feature standardization	Feature standardization implementation?
		Validation method	Validation methods in the development process?
		Preprocessing technique	Selection of preprocessing techniques?
TM.5	Assessment techniques	Data division	Ratio and/or proportion of data division
		Performance metrics	Name and value of measurement

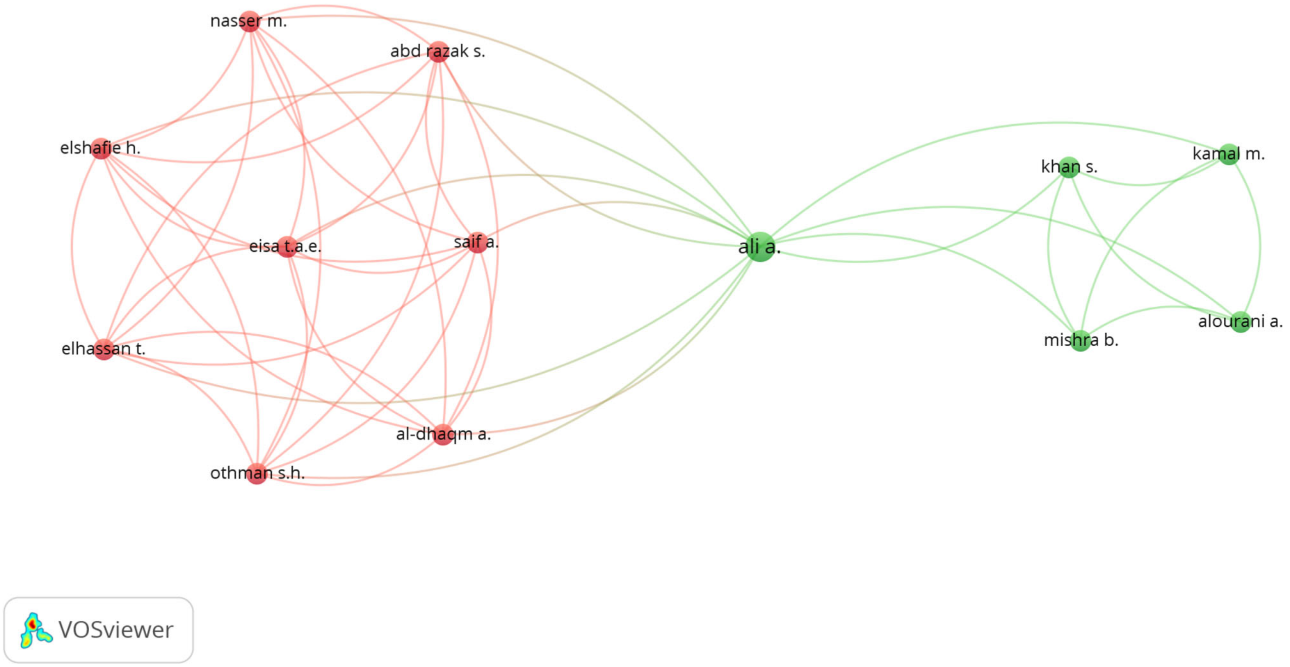


Fig. 2 Map analysis of co-authorship of authors. Shows the analysis of the connections between authors based on co-authorship of publications. Produced with VOSviewer.

In Cluster 13 (light brown), the article by Pourhabibi T. has the greatest number of citations at 102, suggesting that he has been relevant in the research on financial fraud detection. Finally, in Cluster 14 (purple), the articles by Seera M. have 63 citations and 2 links. The article by Ileberi E. has 11 citations and 1 link. Both articles have a small number of citations, indicating a lower influence on the topic.

In conclusion, clusters 2, 4, and 11 are the most relevant in this literature review. The articles by Sahin, Huang, Kim, Dutta, and Pumsirirat are the most influential ones in the research on financial fraud detection through the application of ML models.

Sources. The information presented in Fig. 4 is the result of a clustering analysis of the articles resulting from the literature

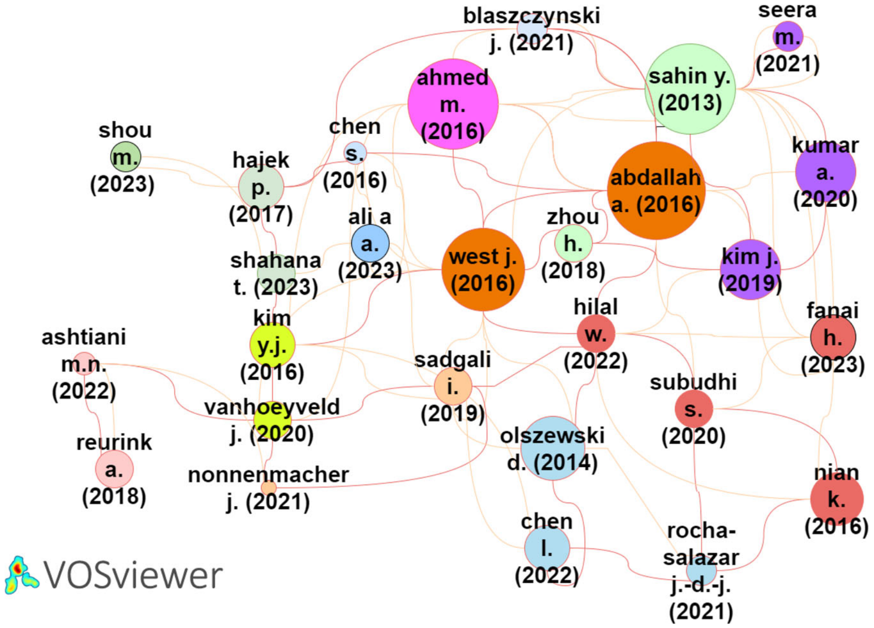


Fig. 3 Analysis map of bibliographic linkage by articles. Depicts the connections between articles based on their bibliographic references. Produced with VOSviewer.

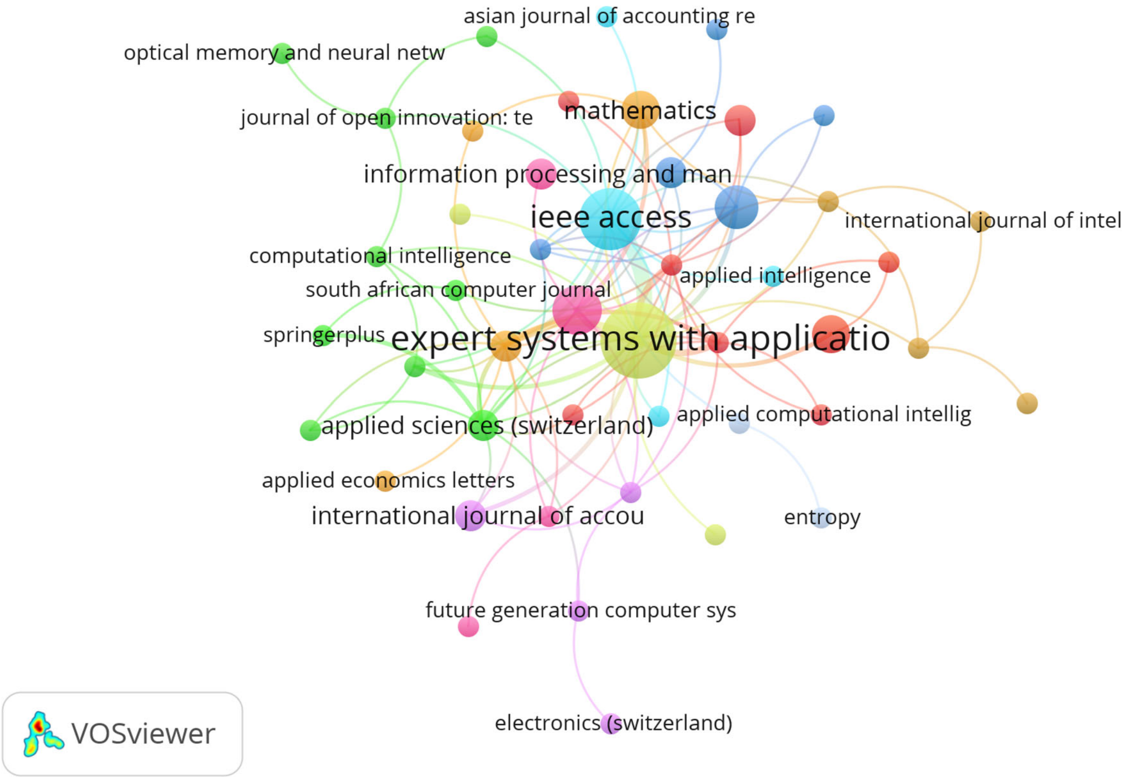

asian journal of accounting re
optical memory and neural netw
journal of open innovation: te
mathematics
information processing and man
ieee access
international journal of intel
computational intelligence
applied intelligence
south african computer journal
springerplus
expert systems with applicatio
applied sciences (switzerland)
applied computational intellig
applied economics letters
international journal of accou
entropy
future generation computer sys
electronics (switzerland)
VOSviewer

Fig. 4 Analysis map of bibliographic linkage of journals. Shows the relationship between different scientific journals based on bibliographic links. Produced with VOSviewer.

review on financial fraud detection by implementing ML models. In total, 48 items were identified and grouped into 12 clusters. The links between the items were 100, with a total link strength of 123.

The following is a description of each cluster with its respective number of items, links, and total link strength (the number of times a link appears between two items and its strength):

Cluster 1 (6 articles—red): This cluster includes journals such as *Computers and Security*, *Journal of Network and Computer Applications*, and *Journal of Advances in Information Technology*. The total number of links is 27, and the total link strength is 32.

Cluster 2 (6 articles—dark green): This cluster includes articles from *Technological Forecasting and Social Change*, *Journal of Open Innovation: Technology, Market, and Complexity*, and

Global Business Review. The total number of links is 18, and the total link strength is 19.

Cluster 3 (5 articles—dark blue): This cluster includes articles from the *International Journal of Advanced Computer Science and Applications*, *Decision Support Systems*, and *Sustainability*. The total number of links is 19, and the total link strength is 20.

Cluster 4 (4 articles—dark yellow): This cluster includes articles from *Expert Systems with Applications* and *Applied Artificial Intelligence*. The total number of links is 26, and the total link strength is 45.

Cluster 5 (4 articles—purple): This cluster includes articles from *Future Generation Computer Systems* and the *International Journal of Accounting Information Systems*. The total number of links is 15, and the total link strength is 16.

Cluster 6 (4 articles—dark blue): This cluster includes articles from *IEEE Access* and *Applied Intelligence*. The total number of links is 18, and the total link strength is 26.

Cluster 7 (4 articles—orange): This cluster includes articles from *Knowledge-Based Systems and Mathematics*. The total number of links is 23, and the total link strength is 29.

Cluster 8 (4 articles—brown): This cluster includes articles from the *Journal of King Saud University—Computer and Information Sciences* and the *Journal of Finance and Data Science*. The total number of links is 13, and the total link strength is 13.

Cluster 9 (4 articles—light purple): This cluster includes articles from the *International Journal of Digital Accounting Research* and *Information Processing and Management*. The total number of links is 2, and the total link strength is 2.

The clusters represent groups of related articles published in different academic journals. Each cluster has a specific number of articles, links, and total link strength. These findings provide an overview of the distribution and connectedness of articles in the literature on financial fraud detection using ML models. Further, clustering helps identify patterns and common thematic areas in the research, which may be useful for future researchers seeking to explore this field.

Clusters 1, 4, and 7 indicate a greater number of stronger articles and links. These clusters encompass articles from *Computers and Security*, *Expert Systems with Applications*, and *Knowledge-Based Systems*, which are important sources for the SLR on financial fraud detection through the implementation of ML models.

Countries. The analysis presented indicates the number of documents related to research in different countries and territories. In this case, a list of 50 countries/territories and the number of documents related to the research conducted in each of them is presented. China leads with the highest paper count at 18, followed by India at 13 and Saudi Arabia and Canada at 9 each. Canada, Malaysia, Pakistan, South Africa, the United Kingdom, France, Germany, and Russia have similar research outputs with 4–9 papers. Sweden and Romania have 1 or 2 research papers, indicating limited scientific research output.

The presence of little-known countries such as Armenia, Costa Rica, and Slovenia suggests ongoing research in places less common in the academic world. From that point on, the number of papers has gradually decreased.

The production of papers is geographically distributed across countries from different continents and regions. However, more research exists on the subject from countries with developed and transition economies, which allows for a greater capacity to conduct research and produce papers.

Figure 5, sourced from Scopus's "Analyze search results" option, depicts countries with their respective number of published papers on the topic of financial fraud detection through ML models.

The above shows the diversity of countries involved in the research, where China leads the number of studies with 18 papers, followed by India with 13 and Saudi Arabia and Canada each with 9 papers. The other countries show little production, with less than 7 publications, which indicates an emerging topic of interest for the survival of companies that must prevent and detect different financial frauds using ML techniques.

Trends. The most relevant keywords in the review of literature on financial fraud detection implementing ML models include the following:

In Cluster 1, the most relevant keywords are "decision trees" (13 repetitions), "support vector machine (SVM)" (11 repetitions), "machine-learning" (10 repetitions), and "credit card fraud detection" (9 repetitions). A special focus has been placed on the topic of artificial intelligence (ML), in addition to algorithms and/or supervised learning models such as decision trees, support vector machines, and credit card fraud detection.

In Cluster 2, the most relevant keywords are "crime" (46 repetitions), "fraud detection" (43 repetitions), and "learning systems" (13 repetitions). These terms reflect a broader focus on financial fraud detection, where the aspects of crime in general, fraud detection, and learning systems used for this purpose have been addressed.

In Cluster 3, the most relevant keywords are "Finance" (19 repetitions), "Data Mining" (18 repetitions), and "Financial Fraud" (12 repetitions). These keywords indicate a focus on the financial industry, where data mining is used to reveal patterns and trends related to financial fraud.

In Cluster 4, the most relevant keywords are "Machine Learning" (45 repetitions), "Anomaly Detection" (16 repetitions), and "Deep Learning" (11 repetitions). They reflect an emphasis on the use of traditional ML and deep learning techniques for anomaly detection and financial fraud detection.

In general, the different clusters indicate the most relevant keywords in the SLR on financial fraud detection through ML models. Each cluster presents a specific set of keywords reflecting the most relevant trends and approaches in this field of research (Fig. 6).

GQ2: What types of financial fraud have been identified in ML studies?

Financial fraud is generated by weaknesses in companies' control mechanisms, which are analyzed based on the variables that allow them to materialize. These include opportunity, motivation, self-fulfillment, capacity, and pressure. Some of these are comprehensively analyzed by Donald Cressey through the fraud theory approach. The lack of modern controls has led organizations to use ML in response to this major problem. According to the findings of the Global Economic Crime and Fraud Survey 2022–2023, which gathered insights from 1,028 respondents across 36 countries worldwide, instances of fraud within these companies have caused a financial loss of approximately 10 million dollars (PricewaterhouseCoopers, 2022).

Referring to the concept of fraud, as outlined in international studies (Estupiñán Gaitán, 2015; Márquez Arcila, 2019; Montes Salazar, 2019) and the guidelines of the American Institute of Certified Public Accountants, it is an illegal, intentional act in which there is a victim (someone who loses a financial resource) and a victimizer (someone who obtains a financial resource from the victim). Thus, the proposed classification includes corporate fraud and/or fraud in organizations, considering that the purpose is to misappropriate the capital resources of an entity or

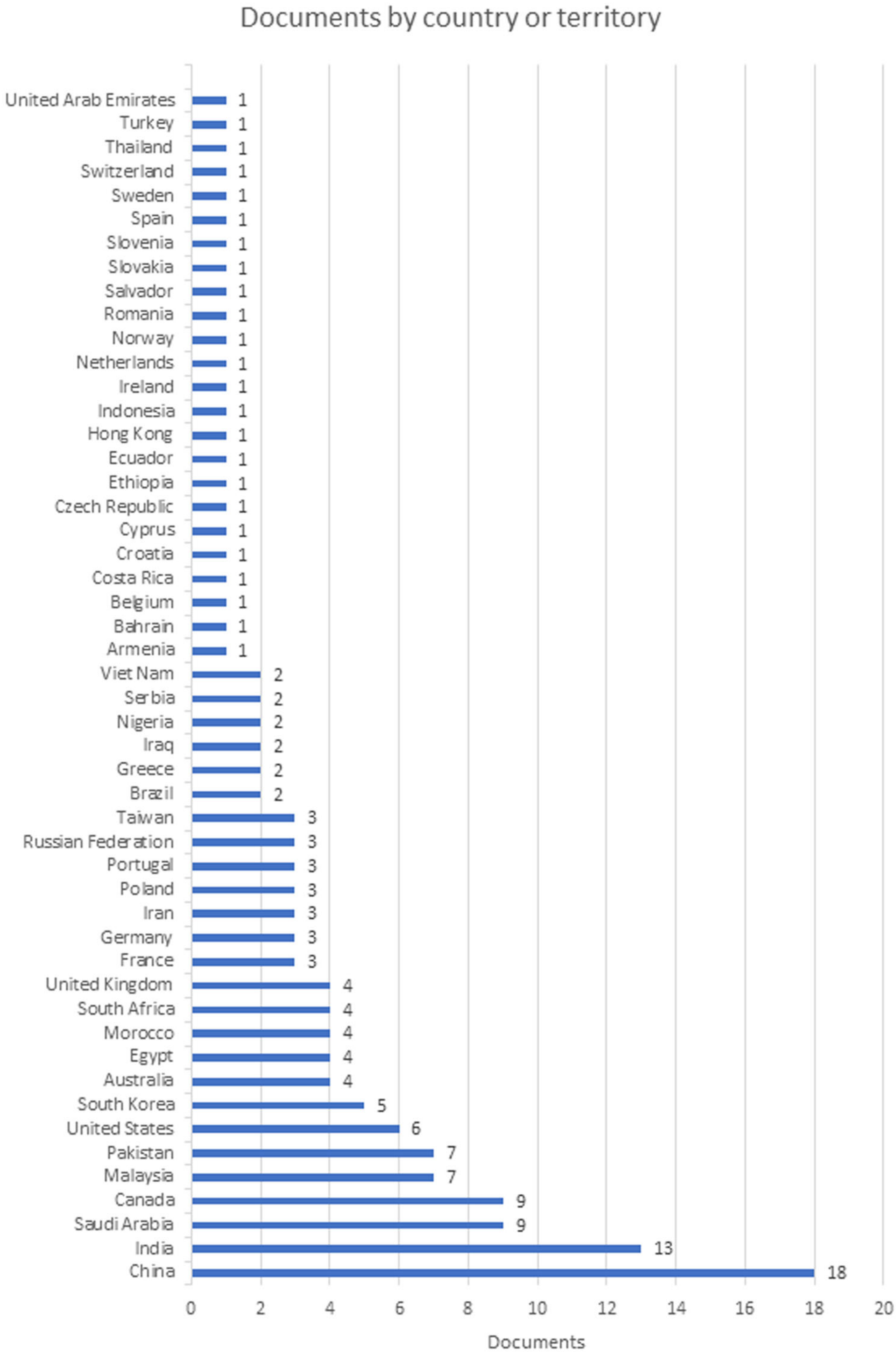


Fig. 5 Number of papers published per country. Represents the number of scientific publications in the study area classified by country. Produced with VOSviewer.

individual: cash, bank accounts, loans, bonds, stocks, real estate, and precious metals, among others.

In this SLR study, we have considered fraud classifications by authors of 86 articles, which encompass experiments. We have excluded the 18 SLR articles from our analysis. The types presented in Table 7 follow the holistic view of the authors of the research for a better understanding of the subject of financial fraud, considering whether it is internal or external fraud.

Table 7 highlights the diverse types of frauds, and the research works on them. According to the classification, external frauds correspond to those performed by stakeholders outside the company. This study's findings show that 54% of the analyzed articles investigate external fraud, among which the most important studies are on credit card loan fraud, followed by insurance fraud, using supervised and unsupervised ML techniques for their detection.

In research works (Kumar et al., 2022) analyzing credit card fraud, attention is drawn to the importance of prevention through the behavioral analysis of customers who acquire a bank loan and identifying applicants for bad loans through ML models. The

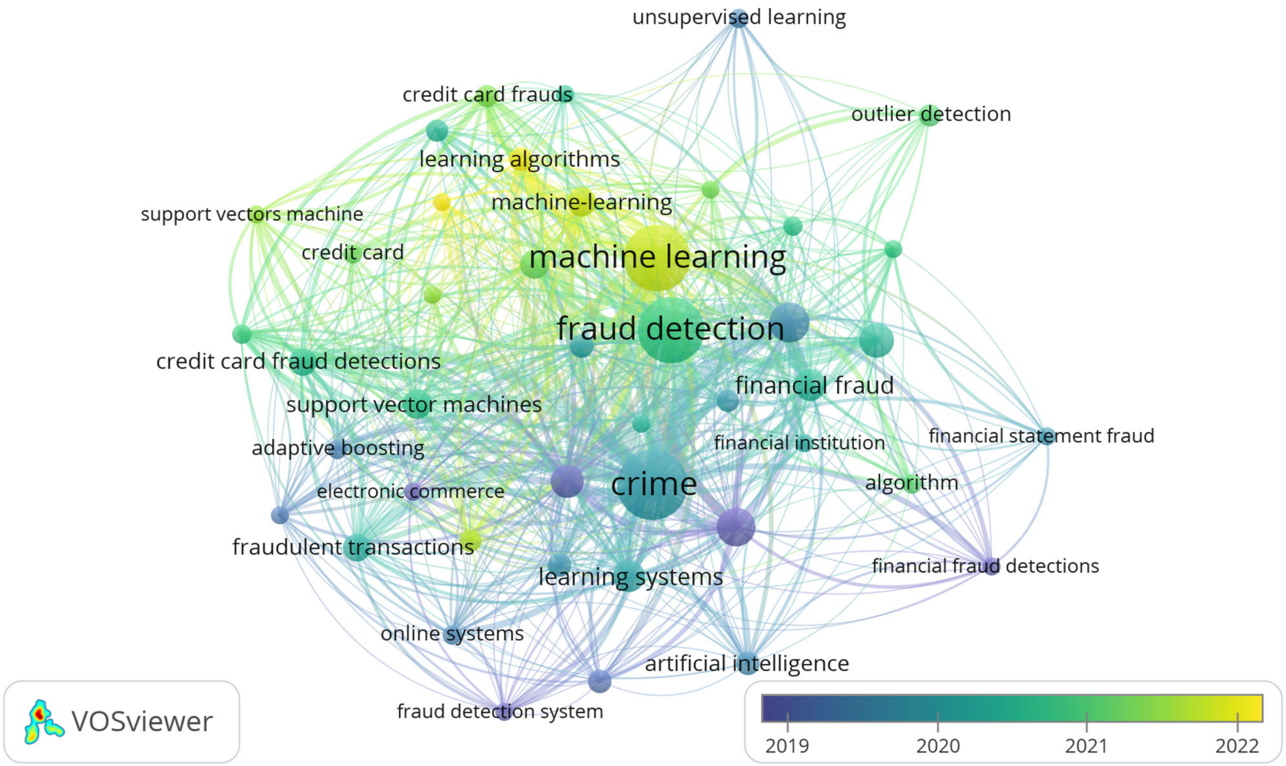


Fig. 6 Keyword co-occurrence map. Shows the relationships between keywords based on their co-occurrence in the literature reviewed. Produced with VOSviewer.

datasets used in these fraud studies have covered transactions performed by credit card holders (Alarfaj et al., 2022; Baker et al., 2022; Hamza et al., 2023; Madhurya et al., 2022; Ounacer et al., 2018; Sahin et al., 2013), while other research works have covered master credit card money transactions in different countries (Wu et al., 2023) and fraudulent transactions gathered from 2014 to 2016 by the international auditing firm Mazars (Smith and Valverde, 2021).

The second major type of external fraud is insurance fraud, which is classified as fraud in health insurance programs involving practices such as document forgery, fraudulent billing, and false medical prescriptions (Sathya and Balakumar, 2022; Van Capelleveen et al., 2016) and automobile insurance fraud involving fraudulent actions between policyholders and repair shops, who mutually rely on each other to obtain benefits (Aslam et al., 2022; Nian et al., 2016; Subudhi and Panigrahi, 2020); as a result of the issues they face, insurance companies have developed robust models using ML.

As regards internal fraud, caused by an individual within the company, 46% of studies have analyzed this type, with financial statement fraud, money laundering fraud, and tax fraud standing out. The studies show that the investigations are based on information reported by the US Securities and Exchange Commission (SEC) and the stock exchanges of China, Canada, Tehran, and Taiwan, among others. To a considerable extent, the information taken is from the real sector, and very few studies have obtained synthetic information based on the application of different learning models.

The following is a summary of the financial information obtained by the researchers to apply AI models and techniques:

a. *Stock market financial reports*: Fraud in the Canadian securities industry (Lokanan and Sharma, 2022), companies listed on the Chinese stock exchanges (Achakzai and Juan, 2022; Y. Chen and Wu, 2022; Xiuguo and Shengyong, 2022), companies with shares according to the SEC (Hajek and Henriques, 2017; Papík and Papíková, 2022), companies listed on the Tehran Stock Exchange (Kootanaee et al. 2021), companies in the Taiwan Economic Journal Data Bank (TEJ) stock market (S. Chen, 2016; S. Chen et al., 2014), analysis of SEC accounting and auditing publications (Whiting et al., 2012)
b. Wrong financial reporting to manipulate stock prices (Chullamonthon and Tangamchit, 2023; Khan et al., 2022; Zhao and Bai, 2022)
c. Financial data of 2318 companies with the highest number of financial frauds (mechanical equipment, medical biology, media, and chemical industries; Shou et al., 2023), fraudulent financial restatements (Dutta et al., 2017)
d. Data from 950 companies in the Middle East and North Africa region (Ali et al., 2023), analyzing outliers in sampling risk and inefficiency of general ledger financial auditing (Bakumenko and Elragal, 2022), fraudulent intent errors by top management of public companies (Y. J. Kim et al., 2016), reporting of general ledger journal entries from an enterprise resource planning system (Zupan et al., 2020)
e. Synthetic financial dataset for fraud detection (Alwadain et al., 2023).

Studies have analyzed situations involving fraudulent financial statements. In these cases, instances of fraud have already occurred, leading to the creation of financial reports that contain statements with outliers that can be deemed fraudulent intent or errors in financial figures. This raises a reasonable doubt about whether an intent exists with regard to the reporting of unrealistic figures. Notably, once there are parties responsible for the financial information presented to stakeholders, such as organization owners, managers, administrators, accountants, or auditors, it is unlikely for it to be unintentional (an error). In this context, transparency and

Table 7 Fraud typology according to RSL.

References	Type of fraud	Learning approach
Elshaar and Sadaoui (2020)	External fraud. Online payments	Supervised learning
Zhang et al. (2018)	External fraud. Online payments	Supervised learning
Vanini et al. (2023)	External fraud. Online payments	Supervised learning
Sofy et al. (2023)	External fraud—fake job posting	Supervised learning
Aslam et al. (2022)	External fraud—insurance	Supervised and unsupervised learning
Van Capelleveen et al. (2016)	External fraud—insurance	Supervised and unsupervised learning
Subudhi and Panigrahi (2020)	External fraud—insurance	Supervised and unsupervised learning
Nian et al. (2016)	External fraud—insurance	Supervised and unsupervised learning
Sathya and Balakumar (2022)	External fraud—insurance	Supervised and unsupervised learning
Srokosz et al. (2023)	External fraud: online transactions	Unsupervised learning
Vanneschi et al. (2018)	External fraud: payment default	Supervised learning
Ashfaq et al. (2022)	External fraud. Digital transactions	Supervised learning
Xiong et al. (2022)	External fraud. Loan fraud	Supervised learning
Chen and Wu (2022)	External fraud. Loan fraud	Supervised learning
Błaszczyński et al. (2021)	External fraud. Loan fraud	Supervised learning
Kumar et al. (2022)	External fraud. TC loan fraud	Supervised and unsupervised learning
Ileberi et al. (2022)	External fraud. TC loan fraud	Supervised and unsupervised learning
Femila Roseline et al. (2022)	External fraud. TC loan fraud	Supervised and unsupervised learning
Udeze et al. (2022)	External fraud. TC loan fraud	Supervised and unsupervised learning
Baker et al. (2022)	External fraud. TC loan fraud	Supervised and unsupervised learning
Alarfaj et al. (2022)	External fraud. TC loan fraud	Supervised and unsupervised learning
Seera et al. (2021)	External fraud. TC loan fraud	Supervised and unsupervised learning
Wu et al. (2023)	External fraud. TC loan fraud	Supervised and unsupervised learning
Smith and Valverde (2021)	External fraud. TC loan fraud	Supervised and unsupervised learning
Plakandaras et al. (2022)	External fraud. TC loan fraud	Supervised and unsupervised learning
Eshghi and Kargari (2019)	External fraud. TC loan fraud	Supervised and unsupervised learning
Sahin et al. (2013)	External fraud. TC loan fraud	Supervised and unsupervised learning
Madhurya et al. (2022)	External fraud. TC loan fraud	Supervised and unsupervised learning
Bekirev et al. (2015)	External fraud. TC loan fraud	Supervised and unsupervised learning
Lee et al. (2018)	External fraud. TC loan fraud	Supervised and unsupervised learning
Domashova and Kripak (2021)	External fraud. TC loan fraud	Supervised and unsupervised learning
Misra et al. (2020)	External fraud. TC loan fraud	Supervised and unsupervised learning
Benchaji et al. (2021)	External fraud. TC loan fraud	Supervised and unsupervised learning
Fang et al. (2019)	External fraud. TC loan fraud	Supervised and unsupervised learning
Zhou et al. (2018)	External fraud. TC loan fraud	Supervised and unsupervised learning
Khan et al. (2022)	External fraud. TC loan fraud	Supervised and unsupervised learning
Hwang and Kim (2020); Tingfei et al. (2020)	External fraud. TC loan fraud	Supervised and unsupervised learning
Tingfei et al. (2020)	External fraud. TC loan fraud	Supervised and unsupervised learning

Table 7 (continued)

References	Type of fraud	Learning approach
Pumsirirat and Yan (2018)	External fraud. TC loan fraud	Supervised and unsupervised learning
Ounacer et al. (2018)	External fraud. TC loan fraud	Supervised and unsupervised learning
Saragih et al. (2019)	External fraud. TC loan fraud	Supervised and unsupervised learning
Fanai and Abbasimehr (2023)	External fraud. TC loan fraud	Supervised and unsupervised learning
Ileberi et al. (2021)	External fraud. TC loan fraud	Supervised and unsupervised learning
Esenogho et al. (2022)	External fraud. TC loan fraud	Supervised and unsupervised learning
Singh et al. (2022)	External fraud. TC loan fraud	Supervised and unsupervised learning
Malik et al. (2022)	External fraud. TC loan fraud	Supervised and unsupervised learning
Huang et al. (2018)	Internal and external financial fraud	Unsupervised learning
Olszewski (2014)	Internal and external fraud: telecommunications, IT network, and CT fraud	Unsupervised learning
Arévalo et al. (2022)	Internal fraud—illegal appropriation of assets—unauthorized massive payments	Unsupervised learning
Rubio et al. (2020)	Internal fraud—illegal appropriation of assets—unauthorized massive payments	Unsupervised learning
Narsimha et al. (2022)	Internal fraud—illegal appropriation of assets—unauthorized massive payments	Unsupervised learning
Hamza et al. (2023)	Internal fraud—unlawful appropriation of assets—dormant account fraud, smurf fraud and bulk fraud	Supervised learning
Dalal et al. (2022)	Internal fraud: illegal appropriation of assets—financial payments	Supervised learning
Kim et al. (2019)	Internal fraud. Corruption	Unsupervised learning
Bakumenko and Elragal (2022); Chen and Wu (2022)	Internal fraud. Financial statement fraud	Supervised and unsupervised learning
Lei et al. (2022)	Internal fraud. Financial statement fraud	Supervised and unsupervised learning
Zupan et al. (2020)	Internal fraud. Financial statement fraud	Supervised and unsupervised learning
Chen and Wu (2022);	Internal fraud. Financial statement fraud	Supervised and unsupervised learning
Hajek and Henriques (2017)	Internal fraud. Financial statement fraud	Supervised and unsupervised learning
Xiuguo and Shengyong (2022)	Internal fraud. Financial statement fraud	Supervised and unsupervised learning
Papík and Papíková (2022)	Internal fraud. Financial statement fraud	Supervised and unsupervised learning
Chen et al. (2014)	Internal fraud. Financial statement fraud	Supervised and unsupervised learning
Kootanaee et al. (2021)	Internal fraud. Financial statement fraud	Supervised and unsupervised learning
Chen, (2016)	Internal fraud. Financial statement fraud	Supervised and unsupervised learning
Shou et al. (2023)	Internal fraud. Financial statement fraud	Supervised and unsupervised learning
Zhao and Bai (2022)	Internal fraud. Financial statement fraud	Supervised and unsupervised learning
Lokanan et al. (2019)	Internal fraud. Financial statement fraud	Supervised and unsupervised learning
Kim et al. (2016)	Internal fraud. Financial statement fraud	Supervised and unsupervised learning
Dutta et al. (2017)	Internal fraud. Financial statement fraud	Supervised and unsupervised learning
Whiting et al. (2012)	Internal fraud. Financial statement fraud	Supervised and unsupervised learning
Alwadain et al. (2023)	Internal fraud. Financial statement fraud	Supervised and unsupervised learning
Ali et al. (2023)	Internal fraud. Financial statement fraud	Supervised and unsupervised learning
Achakzai and Juan (2022)	Internal fraud. Financial statement fraud	Supervised and unsupervised learning

Table 7 (continued)

References	Type of fraud	Learning approach
Lokanan and Sharma (2022)	Internal fraud. Financial statement fraud—investment fraud.	Supervised learning
Chullamonthon and Tangamchit (2023)	Internal fraud. Financial statement fraud—stock price manipulation.	Supervised learning
Khan et al. (2022)	Internal fraud. Financial statement fraud—stock price manipulation.	Supervised learning
Savić et al. (2022)	Internal fraud. Fraud—illegal appropriation of assets—tax appropriation of taxes	Supervised and unsupervised learning
Vanhoeyveld et al. (2020)	Internal fraud. Fraud—illegal appropriation of assets—tax appropriation of taxes	Supervised and unsupervised learning
Baghdasaryan et al. (2022)	Internal fraud. Fraud—illegal appropriation of assets—tax appropriation of taxes	Supervised and unsupervised learning
Domashova and Kripak (2022)	Internal fraud. Illegal appropriation of assets—atypical customer transactions	Supervised learning
Moreira et al. (2022)	Internal fraud. Illegal appropriation of assets.	Supervised learning
Alsuwailem et al. (2022)	Internal fraud. Illicit proceeds money laundering	Supervised learning
Ti et al. (2022)	Internal fraud. Illicit proceeds money laundering	Supervised learning
Lokanan (2022)	Internal fraud. Illicit proceeds money laundering	Supervised learning
Rocha-Salazar et al. (2021)	Internal fraud. Illicit proceeds money laundering	Supervised learning
Usman et al. (2023)	Internal fraud. Illicit proceeds money laundering	Supervised learning

explainability are essential so as to ensure fairness in decisions, thus avoiding bias and discrimination based on prejudiced data (Rakowski et al., 2021).

Because of its significance, the information reported in financial statements is vital for investigations. Studies have indicated substantial amounts of data extracted from the financial reports of regulatory bodies such as stock exchanges and auditing firms. These entities use the data to establish the existence of fraud and its types through predictive models that use ML techniques. Thus, they require financial data such as dates, the third party affected, user, debit or credit amount, and type of document, among other aspects involving an accounting record. This information aids in identifying the possible impact in terms of lower profits and the perpetrator and/or perpetrators to gather sufficient evidence and file criminal proceedings for the financial damage caused.

Moreover, investigations concerning money laundering fraud and/or money laundering, the second most investigated internal fraud type, encompass the reports of natural and legal persons exposed by the Financial Action Task Force in countries such as the Kingdom of Saudi Arabia (Alsuwailem et al., 2022), transactions from April to September 2018 from Taiwan's "T" bank and the account watch list of the National Police Agency of the Ministry of Interior (Ti et al., 2022), money laundering frauds in Middle East banks (Lokanan, 2022), transactions of financial institutions in Mexico from January 2020 (Rocha-Salazar et al., 2021), and synthetic data of simulated banking transactions (Usman et al., 2023).

Concerns regarding the entry of proceeds from money laundering into an organization have been articulated in relation to the financial damage it causes to the country. At the macroeconomic level, these activities negatively affect financial stability, distorting the prices of goods and services. Moreover, such activities disrupt markets, making it difficult to make efficient financial decisions. At the microeconomic level, legitimate businesses face unfair competition with companies using illegal money, which may lead to higher unemployment levels. Furthermore, money laundering has a social impact because it affects the security and welfare of society.

Thus, some research works (Alsuwailem et al., 2022) have indicated the need to implement ML models for promoting anti-money laundering measures. For instance, in Saudi Arabia, money from illicit drug trafficking, corruption, counterfeiting, and product piracy have entered the country. The measures to be taken are categorized according to the three stages of money laundering: placement, layering (also known as concealment), and integration. These include new legal regulations against money laundering, staff training, customer identification and validation, reporting of suspicious activities, and documentation and storage of relevant data (Bolgorian et al., 2023).

Regarding the 7.5% incidence of internal fraud, specifically categorized as tax fraud resulting from tax evasion, the studies have analyzed tax returns on income and/or profits of legal persons and/or individuals from the Serbian tax administration during 2016–2017 (Savić et al., 2022). Studies have encompassed periodic value-added tax (VAT) returns, together with the anonymous list of clients for the tax year 2014 obtained from the Belgian tax administration (Vanhoeyveld et al., 2020) and income tax and VAT taxpayers registered and provided by the State Revenue Committee of the Republic of Armenia in 2018 (Baghdasaryan et al., 2022). These studies hold great relevance for tax administrations using different strategies to minimize the impact of fraud resulting from tax evasion. Tax evasion reduces the government's ability to collect revenue, directly affecting government finances and causing budget deficits, thereby increasing public debt.

GQ3: Which ML models were implemented to detect financial fraud in the datasets?

Given that ML is a key tool to extract meaningful information and make informed decisions, this study analyzes the most widely used ML techniques in the field of financial fraud detection. It takes as reference 86 experimental articles, excluding 18 SLR articles. In these articles, the most commonly used trends and approaches in the implementation of ML techniques in financial fraud detection were identified.

For the analysis, the pattern of frequency of use of ML models was observed. Several of them have been prominent because of their popularity and implementation in detecting financial fraud (Fig. 7). Some of the most widely used models include long-short term memory (LSTM) with 7 mentions, autoencoder with 10 mentions, XGBoost with 13 mentions, *k*-nearest neighbors (KNN) with 14 mentions, artificial neural network (ANN) with 17 mentions, NB with 19 mentions, SVM with 29 mentions, DT with 29 mentions, LR with 32 mentions, and RF with 34 mentions.

The LSTM model is a recurrent neural network used for sequence processing, especially for tasks concerning natural language processing (Chullamonthon and Tangamchit, 2023; Esenogho et al., 2022; Femila Roseline et al., 2022). Moreover,

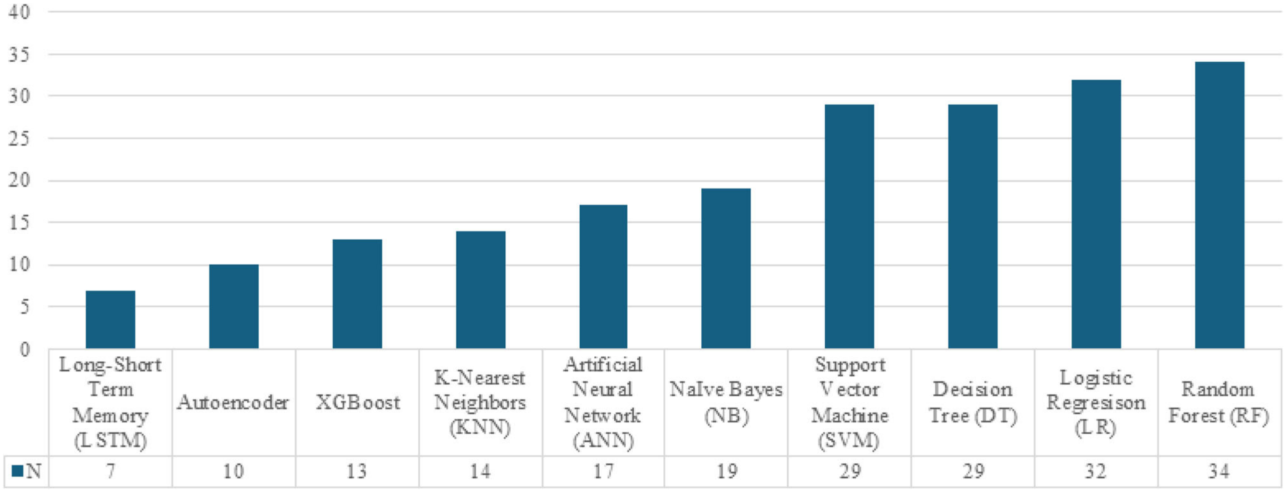


Fig. 7 Main machine learning models used for financial fraud detection. Illustrates the most common machine learning models in financial fraud detection. Authors' own elaboration.

autoencoders are models used for data compression and decompression. These models are useful in dimensionality reduction applications (Misra et al., 2020; Srokosz et al., 2023). XGBoost is a library combining multiple weak DT models, offering a scalable and efficient solution in classification and regression tasks (Dalal et al., 2022; Udeze et al., 2022).

KNN and ANN are widely used models in various ML applications. KNN is based on neighbor closeness, and ANN is inspired by human brain functioning. NB is a probabilistic algorithm commonly used in text classification and data mining (Ashtiani and Raahemi, 2022; Lei et al., 2022; Shahana et al., 2023).

SVM, DT, LR, and RF, the most commonly mentioned models, are used in a wide range of classification and regression applications. These models are prominent because of their effectiveness and applicability to different scenarios, such as credit card loan fraud (external fraud) and financial statement fraud (internal fraud).

The most frequently used ML techniques are supervised learning (56.73%); unsupervised learning (18.29%), a combination of supervised and unsupervised learning (15.38%), a combination of supervised and deep learning (2.88%), and mathematical approach, supervised, and semi-supervised learning (0.96%). Figure 8 presents the ML techniques in the literature reviewed and indicates the number of times each type of technique is applied. Some articles applied several ML methods, in which the algorithms are mainly classified according to the learning method. In this case, there are four main types: supervised, semi-supervised, unsupervised, and deep learning.

Supervised learning is the most widely used technique, with 56.73% of citations in financial fraud studies. In this approach, labeled training data are used, where the expected outputs are known and a model is built that can make higher-accuracy predictions on new unlabeled data. Common examples of supervised learning techniques include the models of LR, SVM, DT, RF, KNM, NB, and ANN.

Moreover, unsupervised learning constitutes 18.27% of the mentions. The technique focuses on discovering patterns in the data without knowing data with labels and/or types for training. Some of these include DBSCAN, autoencoder, and isolation forest (IF).

The combination of supervised, unsupervised, and semi-supervised learning is used with a frequency of 1.92%. This technique and/or approach combines elements of supervised and unsupervised learning, using both labeled and unlabeled data to train the models. It is also used when labeled data are scarce or expensive to obtain; thus, the aim is to take advantage of unlabeled information to improve model performance.

Finally, supervised and deep learning represents 2.88% of the mentions. It is based on deep neural networks with multiple neurons and hidden layers to learn complex data representations. It has achieved remarkable developments in areas such as image processing, voice recognition, and machine translation.

Specific questions (SQ)

SQ1: What datasets were used by implementing ML models for financial fraud detection?

First, the data structure and fraud types may vary with the collection of datasets. The performance of fraud detection models may be affected by variations in the number of instances and attributes selected. Therefore, investigating the datasets and their characteristics is relevant, as data differ in terms of data type (number, text) and the data source from which they were obtained (synthetic and/or real), as can be observed in Fig. 9.

Credit card fraud detection. The dataset was created by the Machine Learning group at Université Libre de Bruxelles. It encompasses anonymized credit card transactions labeled as fraudulent or genuine. The transactions were performed in September 2013 over two days by European cardholders; a record of only 492 frauds out of 284,807 transactions is highly unbalanced because the positive types (frauds) represent only 0.172% of all transactions (Machine Learning Group, 2018).

The characteristics of the set encompass numerical variables resulting from a principal component analysis (PCA) transformation. For confidentiality, the original features of the data have not been disclosed. Features V1, V2…, V28 have been the main components obtained through PCA. The only features that have not transformed with PCA include "Time," which denotes the seconds elapsed between each transaction. "Amount" denotes the transaction amount. The "Class" feature is the response variable, taking 1 as the value in case of fraud and 0 (no fraud) otherwise.

This dataset has been used by 15 authors in their papers, who have applied different financial fraud detection techniques (Alarfaj et al., 2022; Baker et al., 2022; Fanai and Abbasimehr, 2023; Fang et al., 2019; Femila Roseline et al., 2022; Hwang and

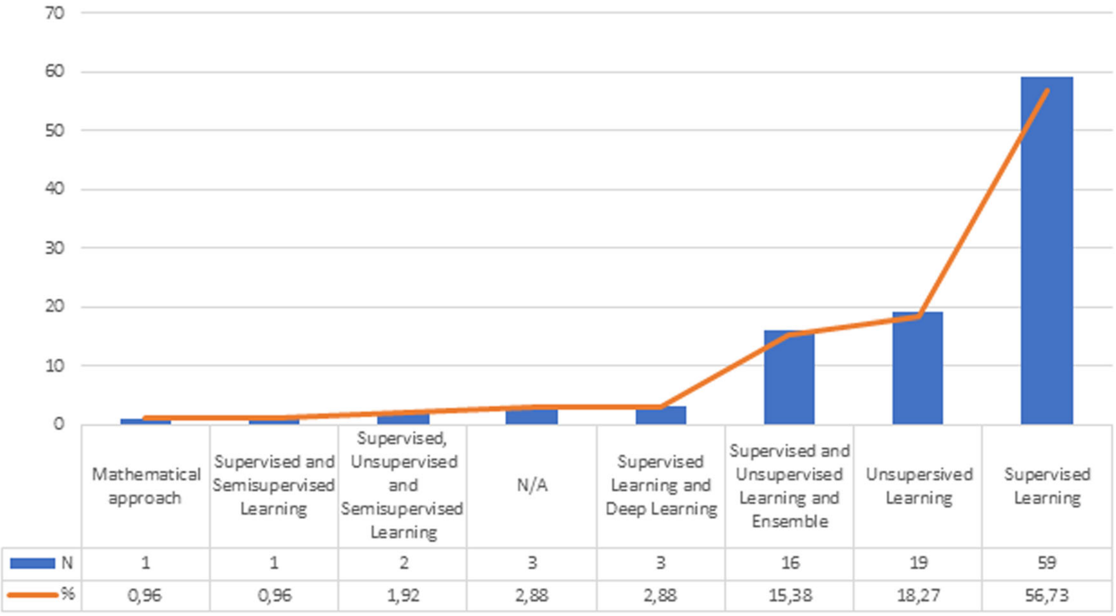


Fig. 8 Approaches used in the experiments. Shows the different experimental approaches used in the study. Authors' own elaboration.

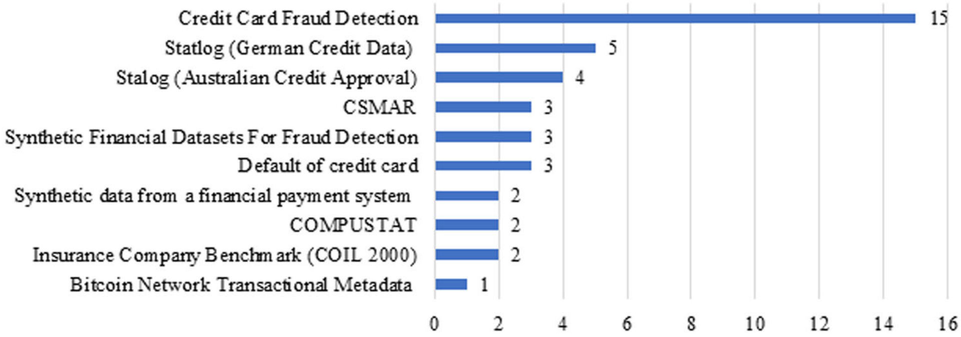


Fig. 9 Datasets for financial fraud detection. Depicts the datasets used in the research on financial fraud detection. Authors' own elaboration.

Kim, 2020; Ileberi et al., 2021, 2022; Khan et al., 2022; Misra et al., 2020; Ounacer et al., 2022).

Statlog (German credit data). The dataset was proposed by Professor Hofmann to the UC Irvine ML repository on November 16, 1994, for facilitating credit rating (Hofmann, 1994). It mainly aims to determine whether a person presents a favorable or unfavorable credit risk (binary rating). The set is multivariate, which implies that it contains many attributes used in credit rating. These attributes include information on existing current account status, credit duration, credit history, and credit purpose and amount, among others. In total, there are 20 attributes describing several characteristics of individuals and contains 1000 instances; it has been widely used in research related to credit rating (Esenogho et al., 2022; Fanai and Abbasimehr, 2023; Lee et al., 2018; Pumsirirat and Yan, 2018; Seera et al., 2021).

Stalog (Australian credit approval). The dataset belongs to the UC Irvine ML repository and was created by Ross Quinlan in 1997. It focuses on credit card applications within the financial field (Quinlan, 1997). It has a total of 690 instances and 14 attributes of which 6 are numeric of type integer/actual and 8 are categorical; consequently, its data characteristics are multivariate—that is, it contains multiple variables and/or attributes. Several studies have used the ensemble data (Lee et al., 2018; Pumsirirat and Yan, 2018; Seera et al., 2021; Singh et al., 2022).

China Stock Market and Accounting Research. The China Stock Market and Accounting Research (CSMAR) Database contains financial reports and violations of CSMAR. It provides information on China's stock markets and the financial statements of listed companies; the data were collected between 1998 and 2016 from publicly funded companies (CSMAR, 2022). It includes fraudulent and non-fraudulent companies committing several types of fraud, such as showing higher profits and/or earnings, fictitious assets, false records, and other irregularities in financial reporting.

The set comprises 35,574 samples, including 337 annual fraud samples of companies in the Chinese stock market. This is selected as a data source to illustrate the financial statement information of listed companies in three studies (Achakzai and Juan, 2022; Y. Chen and Wu, 2022; Shou et al., 2023).

Synthetic financial datasets for fraud detection. It was generated by the PaySim mobile money simulator using aggregated data from a private dataset deriving from one month of financial records from a mobile money service in an African country (López-Rojas, 2017). The original records were provided by a multinational company offering mobile financial services in more than 14 countries worldwide. The dataset has been used in numerous studies (Alwadain et al., 2023; Hwang and Kim, 2020; Moreira et al., 2022).

The synthetic dataset provided is a scaled-down version, representing a quarter of the original dataset. It was made available for Kaggle. It constitutes 6,362,620 samples, with 8213 fraudulent transaction samples and 6,354,407 non-fraudulent transactions. It includes several attributes related to mobile money transactions: transaction type (cash-in, cash-out, debit, payment, and transfer); transaction amount in local currency; customer information (customer conducting the transaction and transaction recipient); initial balances before and after the transaction; and fraudulent behavior indicators (isFraud and isFlaggedFraud). These attributes indicate a binary classification.

Default of credit card clients. It was created by I-Cheng Yeh and introduced on January 25, 2016, and is available in the UC Irvine ML repository (Yeh, 2016). The dataset, which is used for classification tasks, focuses on the case of defaulted payments of credit card customers in Taiwan in the business area. Moreover, it is a multivariate dataset with 30,000 instances and 24 attributes. They include attributes such as the amount of credit granted, payment history, and statement records spanning April through September 2005. This data source is selected in studies such as those by Esenogho et al. (2022), Pumsirirat and Yan (2018), and Seera et al. (2021).

Synthetic data from a financial payment system. Edgar Lopez Rojas created the dataset in 2017. The synthetic data were generated in the BankSim payment simulator. It is based on a sample of transactional data provided by a bank in Spain (López-Rojas, 2017). It includes the following characteristics: step, customer ID, age, gender, zip code, merchant ID, zip code of merchant, category of purchase, amount of purchase, and fraud status. It comprises 594,643 transactions, of which ~1.2% (7200) were labeled as fraud and the rest (587,443) were labeled as genuine, and it was processed as a binary classification problem. The dataset has been used in several investigations (Esenogho et al., 2022; Pumsirirat and Yan, 2018; Seera et al., 2021).

COMPUSTAT. This dataset is a financial and economic information and research database (Compustat, 2022). It contains characteristics related to various aspects of companies, such as asset quality, revenues earned, administrative and sales expenses, and sales growth, among others. COMPUSTAT collects and stores detailed information on listed companies in the United States and Canada. The set includes information on 61 characteristics and consists of 228 companies, of which half showed fraud in their information while the other half did not present fraud (binary classification), and it is used in studies (Dutta et al., 2017; Whiting et al., 2012).

Insurance Company Benchmark (COIL 2000). This dataset is used in the CoIL 2000 challenge, available at the UC Irvine Machine Learning Repository, created by Peter Van Der Putten. It consists of 9822 instances and 86 attributes containing information about customers of an insurance company and includes data on product use and sociodemographic data (Putten, 2000). It is characterized as multivariate and is used to perform regression/classification tasks by studies using the dataset (Huang et al., 2018; Sathya and Balakumar, 2022).

Bitcoin network transactional metadata. This dataset contains Bitcoin transaction metadata from 2011 to 2013. It was created by Omer Shafiq (Kaggle handle: OmerShafiq) and introduced to the Kaggle online community in 2019. The set comprises 11 attributes and 30,000 instances related to Bitcoin transactions, bitcoin flows, connections between transactions, average ratings, and malicious transactions (Omershafiq, 2019). It is efficient for investigating and analyzing anomalies and fraud detection in Bitcoin transactions (Ashfaq et al., 2022).

SQ2: What were the metrics used to assess the performance of ML models to detect financial fraud?

Based on previous studies (Nicholls et al., 2021; Shahana et al., 2023), the performance of the metrics used in ML models is the last step in determining whether the results align with the problem at hand. The metrics demonstrate the ability to do a specific task, such as classification, regression, or clustering quality, as they allow comparing the performance of models.

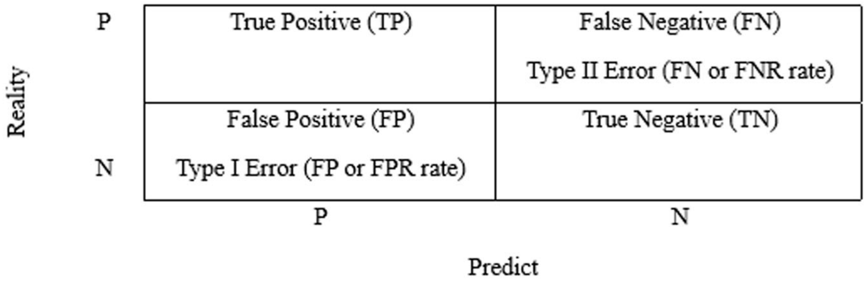
Many evaluation metrics have been used in previous studies, such as precision, sensitivity, recall, accuracy, and area under the curve. These metrics can be calculated using the confusion matrix. Figure 10 compares the target and true values with the predicted ones based on the study by Torrano et al. (2018).

According to previous studies (Shahana et al., 2023; Zhao and Bai, 2022), true positive (TP) projects a positive value (fraud) that matches the true value; true negative (TN) accurately predicts a negative outcome (no fraud); false positive (FP) denotes the predicted positive whose true value is negative (no fraud); and false negative (FN) represents the predicted negative whose true value is positive (fraud). FP and FN represent the misclassification cost, also known as classification model prediction error.

The metrics used to evaluate the effectiveness of supervised ML techniques are as follows. The accuracy metric is the most commonly used (Ramírez-Alpízar et al., 2020). It is defined as the total number or proportion of correct predictions/samples over the total number of records analyzed. Further, it is a method of evaluating the performance of a binary classification model distinguishing between true and false. In Eq. (1), it calculates the accuracy metric.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

The sensitivity metric known as recall (TP or TPR rate) is the ratio of successfully identified fraudulent predictions to the total



		P	N
Reality	P	True Positive (TP)	False Negative (FN) Type II Error (FN or FNR rate)
	N	False Positive (FP) Type I Error (FP or FPR rate)	True Negative (TN)

Fig. 10 Confusion matrix. Presents the confusion matrix generated during the evaluation of the financial fraud detection models. Authors' own elaboration.

number of fraudulent samples. Equation (2) calculates the sensitivity metric.

$$Sensitivity = \frac{TP}{P} \tag{2}$$

The specificity metric (TN rate or TNR) is the percentage of non-fraudulent samples properly designated as non-fraudulent. It is represented in Eq. (3).

$$Specificity = \frac{TN}{N} \tag{3}$$

Accuracy is the ratio of correctly classified fraudulent predictions to the total number of fraudulent predictions. Equation (4) calculates the precision metric.

$$Precision = \frac{TP}{TP + FP} \tag{4}$$

F1-score is a metric that combines accuracy and recall using a weighted harmonic mean (Bakumenko and Elragal, 2022). It is presented in Eq. (5).

$$F1 - Score = \frac{2 * Recall * Precision}{Recall + Precision} \tag{5}$$

Type I error (FP or FPR rate) is the number of legitimate predictions mistakenly labeled as fraudulent as a percentage of all legitimate predictions. The metric is defined in Eq. (6).

$$Type\,I\,error = \frac{FP}{N} = 1 - TN\ rate \tag{6}$$

Type II error (FN or FNR rate) is the proportion of fraudulent samples incorrectly designated as non-fraudulent. Type I and II errors make up the overall error rate. It is defined in Eq. (7).

$$Type\ II\ error = \frac{FP}{NP} = 1 - TP\ rate \tag{7}$$

The area under the curve (AUC), or area under the receiver operating characteristic curve, represents a graphic of TPR versus FPR (Y. Chen and Wu, 2022). AUC values range from 0 to 1; the more accurate an ML model, the higher its AUC value. It is a metric that represents the model's performance when differentiating between two classes.

Following the guidelines in previous studies (Amrutha et al., 2023; García-Ordás et al., 2023; Palacio, 2019), some metrics used to evaluate the effectiveness of unsupervised ML techniques will be defined.

The silhouette coefficient identifies the most appropriate number of clusters; a higher coefficient means better quality with this number of clusters. Equation (8) calculates the metric.

$$s(j) = \frac{y - x}{\max(x, y)} \tag{8}$$

where x denotes the average of the distances of observation j with respect to the rest of the observations of the cluster to which j belongs. Furthermore, y denotes the minimum distance to a different cluster. The silhouette score takes values between -1 and 1. Based on the study by Viera et al. (2023), 1 (correct) represents the assignment of observation j to a good cluster, zero (0) indicates that observation j is between two distinct groups, and -1 (incorrect) indicates that the assignment of j to the cluster is a bad clustering.

The rand index is the similarity measure between two clusters considering all pairs and including those assigned to the same cluster in both the predictions and the true cluster. Equation (9) calculates the index.

$$RI = \frac{TP + TN}{TP + FP + TN + FN} * 100 \tag{9}$$

The Davies–Bouldin metric is a score used to evaluate clustering algorithms. It is defined as the mean value of the samples, represented in Eq. (10).

$$DB = \frac{1}{K}\sum_{i=1}^{k} \max_{j \neq i} \left(\frac{\alpha_i + \alpha_j}{d\left(c_i, c_j\right)}\right) \tag{10}$$

where k denotes the number of groups c_i, c_j, k represents the centroids of cluster i and j, respectively, with $d\left(c_i, c_i\right)$ as the distance between them, while α_i and α_j corresponds to the average distance of all elements in clusters i and j and the distance to their respective c_i and c_j centroids (Viera et al., 2023).

The Fowlkes–Mallows index is defined as the geometric mean between precision and recall, represented in Eq. (11).

$$FM = \sqrt{\frac{TP}{TP + FP} * \frac{TP}{TP + FN}} \tag{11}$$

The cophenetic correlation coefficient is a clustering method to produce a dendrogram (tree diagram). Equation (12) indicates the metric.

$$CPC = \frac{\sum_{i<j}\left(x\left(i,j\right) - \bar{x}\right)\left(t\left(i,j\right) - \bar{t}\right)}{\sqrt{\left[\sum_{i<j}\left(x\left(i,j\right) - \bar{x}\right)^2\right]\left[\sum_{i<j}\left(t\left(i,j\right) - \bar{t}\right)^2\right]}} \tag{12}$$

where $x(i,j) = |x_i - x_j|$ represents the Euclidean distance between the ith and jth points of x. While $t(i,j)$ is the height of the node at which the two points, t_i and t_j, of the dendrogram meet and $\bar{x}$ and $\bar{t}$ are the mean value of $x(i,j)$ and $t(i,j)$.

Discussion and conclusion

Research on the detection of financial fraud by applying ML techniques is a significant topic. On the one hand, fraud directly affects the business world and, on the other hand, detecting it early involves great challenges; this has led to designing tools using AI, such as ML techniques. This study is an SLR using adaptations of the PRISMA and Kitchenham methods to critically analyze and synthesize the study results. Research articles published in Scopus, IEEE Xplore, Taylor & Francis, SAGE, and ScienceDirect were explored. The results were presented in two parts. The first one included a bibliometric study with the open-source software VOSviewer, followed by a discussion of the SLR results.

The bibliometric analysis presented the results of the authors, articles, sources, countries, and most important trends in the literature on financial fraud detection by applying ML, as well as an analysis of fraud types, ML models, and datasets. From the 104 articles dating from 2012 to 2023, several types of fraudulent activities are described, as well as external (e.g., credit cards, insurance) and internal (e.g., financial statements, money laundering) frauds, and a brief report on fraud, in general, is provided. Further, it was possible to extract supervised and unsupervised ML techniques, with the 10 most used models as RF in supervised techniques and autoencoder as an unsupervised technique.

During the literature review on the detection of financial fraud using machine learning models, it became evident that several authors have made significant contributions. However, some stand out more in terms of the number of publications and citations. Some of the most notable ones, Ahmed M. with 318 citations, Ileberi E. with 82, and Chen S. with 84, have made important advances in the field. Others, such as Abdallah A., with only one publication, but with 333 citations, have also made a considerable impact. And although researchers such as Khan S. and Mishra B. have fewer citations, the combined work of all these authors has established a robust knowledge base, providing a deeper understanding of the challenges and opportunities present in financial fraud detection through machine learning techniques.

Consistent with the analysis of the article clusters, clusters 2, 4 and 11 emerge as the most influential in this field with topics of interdisciplinary interest (artificial intelligence/machine learning, accounting, finance), among academics and auditing firms. The SLR evidences that authors in these domains often cooperate when it comes to publication, in turn, studies by (Huang et al., 2018; J. Kim et al., 2019; Sahin et al., 2013; Dutta et al., 2017) are highly cited articles.

Similarly, the leading countries in the research area include China, which has the largest number of published articles, followed by India and Saudi Arabia. The production of articles on the subject was found to be geographically distributed among countries whose economies are developing and are in transition, which indicates a greater capacity for the production of papers and research. In comparison to Ashtiani and Raahemi's (2022) study highlighting the United States, leading with the largest number of papers (18) in the area, followed by China (8) and Greece (7), Al-Hashedi and Magalingam's (2021) posit that India is the top producer of articles with 24, followed by China (14) and the United States (9).

The journals that have accepted the publication of these studies are specifically in the accounting and computer science domain. There is much literature on computers and security, expert systems with applications, and knowledge-based systems on financial fraud detection through ML models, as supported by Al-Hashedi and Magalingam (2021) and Ali et al. (2022). The keywords highlighted in the studies include crime, fraud detection, and ML. These words indicate a central focus on the financial industry, where learning and/or data mining systems help discover patterns or anomalies in financial data, in addition to attractive trends and approaches in the research field.

The literature has indicated articles investigating fraud types, particularly credit card loan fraud and insurance fraud, which are of great interest to the scientific community (Al-Hashedi and Magalingam, 2021; Ali et al., 2022; West and Bhattacharya, 2016). This study has classified the different types of fraud into internal and external, and sub-classifications have been derived. In both types, ML techniques have been used to detect financial fraud—supervised (59 articles), unsupervised (19 articles), supervised and unsupervised (16 articles), and deep learning (3 articles), among others. Most of the studies analyzed have developed binary classification models, that is, fraud or non-fraud. Supervised learning techniques require labeled data, and the most frequently used models are LR, RF, and SVM, among others. In the experiments, the prevalence of metrics such as accuracy, precision, sensitivity, and F1-score are highlighted. For unsupervised learning as a technique, the data do not have a label and focus on discovering new patterns with algorithms such as DBSCAN, autoencoder, and IF, among others. The evaluation with internal metrics was not made in detail. Few studies using semi-supervised learning and deep learning techniques have been highlighted because of the fact that they are novel.

Further, it is found in the trend through the keywords, as the research works address the subject of ML, learning algorithms, deep learning, SVM, fraudulent transactions, and anomaly detection, but it is evident that there is little research on unsupervised learning and deep learning. The scarce use of these techniques may be because of the complexity of the models and the high consumption of computational resources. In the analysis of the 86 experiment articles, few articles were found that used unsupervised techniques. Also, a large part of the datasets used is labeled, which requires further experimentation with models and unlabeled real-world datasets (Ounacer et al., 2018; Pumsirirat and Yan, 2018; Rubio et al., 2020; Van Capelleveen et al., 2016; Vanini et al., 2023). Meanwhile, labeled data are costly because an expert is required for their construction. Thus, more attention has been given to data origin, preprocessing, and feature extraction before training an ML model to increase detection accuracy. Accordingly, it should be emphasized that deep learning models require a thorough design and adjustment compared with previous models. They are quite sensitive to the architecture structure and choice of hyperparameters. Further, the data quality and quantity required is relatively high, so it should be considered in the design stage.

The studies show that the datasets for the experiments were taken from the stock exchanges of China, Canada, the United States, Taiwan, and Tehran, among others. The researchers used ML models to detect financial fraud in credit card loans, highlighting the use of the "Credit Card Fraud Detection" dataset, mentioned 15 times. Also, the performance of ML models can be affected because of the selected set by the number of selected attributes and instances. From the analysis, it was observed that most of the articles use real datasets obtained from existing databases, historical records, or other collection methods, and few studies use synthetic datasets (four articles), which are those generated by modeling or simulation techniques and try to mimic a real dataset.

Still, the integration of real and synthetic datasets enables a comprehensive approach to the problem by providing a basis and complementary information for conclusions and comparisons with other studies on the performance of ML models. Specifically, the datasets used in recent studies and/or articles, spanning from 2012 to 2023, reveal concern related to obsolete data approximately from 1994, which, because of their age, do not provide effective and accurate results in the current context as a result of the new fraud modalities created day after day, with characteristics and behavior patterns that have evolved significantly over time.

The literature review and bibliometric analyses on financial fraud detection using machine learning and its various techniques conducted between 2012 and 2023 show a remarkable evolution in this field. Authors, including Ahmed M., Ileberi E., and Chen S. have made important contributions with a high number of citations. There has been fundamental interdisciplinary collaboration between areas such as artificial intelligence, accounting, finance, and information security, highlighting widely cited studies such as Huang et al. (2018), J. Kim et al. (2019), Sahin et al. (2013), and Dutta et al. (2017). Countries such as China, India and Saudi Arabia leading in publications can be seen, which reflects the global effort of emerging economies. Supervised learning techniques such as Random Forest, and unsupervised ones, like Autoencoder, are the most widely used. Furthermore, the effort and enthusiasm for the use of deep learning, despite its complexity and high computational resource requirements, are evident.

Research mainly uses real datasets such as those from the Chinese, Canadian, US, Taiwanese, and Tehran stock exchanges, with the "Credit Card Fraud Detection" dataset being the most important one. The journals that publish these studies belong both to the accounting area and to computer science, with extensive literature in Computers and Security, Expert Systems with Applications, and Knowledge-Based Systems. While it is true that the accuracy of fraud detection depends on the quality of the data and preprocessing with various algorithms, the need for robust and updated approaches to face new fraud modalities is particularly highlighted.

Limitations and scope for future research. The study had limitations that affected the scope and interpretation of the results.

Although a systematic review was performed, the lack of quantitative support in the data collected is acknowledged. From the 104 articles identified in the SLR, 18 correspond to systematic reviews, which limits the availability of studies with specific details or experiments. This affected the depth of the analysis and the comprehensiveness of the results obtained.

The literature review reveals a predominant emphasis on the banking sector, especially in relation to credit card fraud and insurance fraud. The narrow focus leads to a lack of diversity in the types of fraud studied, excluding internal fraud types such as embezzlement, racketeering, smurfing, defalcation, collusion, signature forgery, and manipulation of accounting documents, among others. The underrepresentation of these other fraud types compromises the generalization of the findings and the applicability of ML models to contexts beyond the banking sector.

The datasets analyzed show a significant deficiency in the representation of fraud types. It can be observed that most of these datasets originated from the main stock exchanges and, additionally, the information used to carry out the experiments is old. This scenario indicates the inclusion of non-contemporary fraud types in the analysis. The limited availability of information on the performance metrics of the unsupervised learning models made it difficult to count the evaluation metrics used to predict financial fraud.

The field of financial fraud detection using ML models offers promising prospects for future research. An area of potential improvement is experimentation with advanced techniques, such as reinforcement learning or deep neural network architectures, to improve the accuracy and efficiency of models, including unsupervised learning. This approach could enable the development of more sophisticated systems capable of identifying complex fraud patterns and dynamically adjusting to the changing strategies of criminals, who are constantly innovating new fraud methods.

Moreover, it is suggested that the applicability of fraud detection systems in contexts other than banking be analyzed by adopting the anomaly approach, which would make it possible to move forward in the detection of fraud in real-time and minimize risks in organizations. It is also proposed that a dataset be created, containing real context information, which is freely accessible and includes new fraud methods to provide the scientific community with an updated dataset.

Data availability

The datasets generated and/or analyzed in this study are available in the Harvard Dataverse repository https://doi.org/10.7910/DVN/CM8NVY.

Received: 15 November 2023; Accepted: 13 August 2024;
Published online: 03 September 2024

References

Abdallah A, Maarof MA, Zainal A (2016) Fraud detection system: a survey. J Netw Comput Appl 68:90–113. https://doi.org/10.1016/j.jnca.2016.04.007

Achakzai MAK, Juan P (2022) Using machine learning meta-classifiers to detect financial frauds. Financ Res Lett 48:102915. https://doi.org/10.1016/j.frl.2022.102915

Ahmed M, Mahmood AN, Islam MdR (2016) A survey of anomaly detection techniques in financial domain. Future Gener Comput Syst 55:278–288. https://doi.org/10.1016/j.future.2015.01.001

Al Ali A, Khedr AM, El-Bannany M, Kanakkayil S (2023) A powerful predicting model for financial statement fraud based on optimized XGBoost ensemble learning technique. Appl Sci 13(4):2272. https://doi.org/10.3390/app13042272

Alarfaj FK, Malik I, Khan HU, Almusallam N, Ramzan M, Ahmed M (2022) Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. IEEE Access 10:39700–39715. https://doi.org/10.1109/ACCESS.2022.3166891

Al-Hashedi KG, Magalingam P (2021) Financial fraud detection applying data mining techniques: a comprehensive review from 2009 to 2019. Comput Sci Rev 40:100402. https://doi.org/10.1016/j.cosrev.2021.100402

Ali A, Abd Razak S, Othman SH, Eisa TAE, Al-Dhaqm A, Nasser Tusneem ME, Elshafie H, Saif A (2022) Financial fraud detection based on machine learning: a systematic literature review. Appl Sci (Switz). https://doi.org/10.3390/app12199637

Alsuwailem AAS, Salem E, Saudagar AKJ (2022) Performance of different machine learning algorithms in detecting financial fraud. Comput Econ. https://doi.org/10.1007/s10614-022-10314-x

Alwadain A, Ali RF, Muneer A (2023) Estimating financial fraud through transaction-level features and machine learning. Mathematics 11(5):1184. https://doi.org/10.3390/math11051184

Amrutha E, Arivazhagan S, Jebarani WSL (2023) Deep clustering network for steganographer detection using latent features extracted from a novel convolutional autoencoder. Neural Process Lett 55(3):2953–2964. https://doi.org/10.1007/s11063-022-10992-6

Arévalo F, Barucca P, Téllez-León I-E, Rodríguez W, Gage G, Morales R (2022) Identifying clusters of anomalous payments in the salvadorian payment system. Lat Am J Cent Bank. 3(1):100050. https://doi.org/10.1016/j.latcb.2022.100050

Ashfaq T, Khalid R, Yahaya A, Aslam S, Alsafari S, Hameed I (2022) A machine learning and blockchain bases efficient fraud detection mechanism. Sensors 22(19):7162. https://doi.org/10.3390/s22197162

Ashtiani MN, Raahemi B (2022) Intelligent fraud detection in financial statements using machine learning and data mining: a systematic literature review. IEEE Access 10:72504–72525. https://doi.org/10.1109/ACCESS.2021.3096799

Aslam F, Hunjra A, Ftiti Z, Louhichi W, Shams T (2022) Insurance fraud detection: evidence from artificial intelligence and machine learning. Res Int Bus Financ. https://doi.org/10.1016/j.ribaf.2022.101744

Baghdasaryan V, Davtyan H, Sarikyan A, Navasardyan Z (2022) Improving tax audit efficiency using machine learning: the role of taxpayer's network data in fraud detection. Appl Artif Intell 36(1). https://doi.org/10.1080/08839514.2021.2012002

Baker MR, Mahmood ZN, Shaker EH (2022) Ensemble learning with supervised machine learning models to predict credit card fraud transactions. Rev Intell Artif. https://doi.org/10.18280/ria.360401

Bakumenko A, Elragal A (2022) Detecting anomalies in financial data using machine learning algorithms. Systems. https://doi.org/10.3390/systems10050130

Bekirev AS, Klimov VV, Kuzin MV, Shchukin BA (2015) Payment card fraud detection using neural network committee and clustering. Optical Mem. Neural Netw 24(3):193–200. https://doi.org/10.3103/S1060992X15030030

Benchaji I, Douzi S, Ouahidi BEl (2021) Credit card fraud detection model based on LSTM recurrent neural networks. J Adv Inf Technol 12(2):113–118. https://doi.org/10.12720/jait.12.2.113-118

Błaszczyński J, de Almeida Filho AT, Matuszyk A, Szeląg M, Słowiński R (2021) Auto loan fraud detection using dominance-based rough set approach versus machine learning methods. Expert Syst Appl 163:113740. https://doi.org/10.1016/j.eswa.2020.113740

Bolgorian M, Mayeli A, Ronizi NG (2023) CEO compensation and money laundering risk. J Econ Criminol 1:100007. https://doi.org/10.1016/j.jeconc.2023.100007

Chen S (2016) Detection of fraudulent financial statements using the hybrid data mining approach. SpringerPlus 5(1):89. https://doi.org/10.1186/s40064-016-1707-6

Chen S, Goo Y-JJ, Shen Z-D (2014) A hybrid approach of stepwise regression, logistic regression, support vector machine, and decision tree for forecasting fraudulent financial statements. Sci World J 2014:1–9. https://doi.org/10.1155/2014/968712

Chen Y, Wu Z (2022) Financial fraud detection of listed companies in China: a machine learning approach. Sustainability 15(1):105. https://doi.org/10.3390/su15010105

Chullamonthon P, Tangamchit P (2023) Ensemble of supervised and unsupervised deep neural networks for stock price manipulation detection. Expert Syst Appl 220:119698. https://doi.org/10.1016/j.eswa.2023.119698

Compustat (2022) Compustat. S&P Global Market Intelligence. https://www.marketplace.spglobal.com/en/datasets?cq_cmp=9778467255&cq_plac=&cq_net=g&cq_pos=&cq_plt=gp&utm_source=google&utm_medium=cpc&utm_campaign=DMS_Marketplace_Search_Google&utm_term=&utm_content=586436401424&_bt=586436401424&_bk=&_bm=&_bn=g&_bg=133704002389&gclid=Cj0KCQjw4s-kBhDqARIsAN-ipH3TguUoVohfDZgD65fjvKomc6BBgJ3uA9zP95m6u4vOs5yG7_L7w2UaAnnvEALw_wcB

CSMAR (2022) China Stock Market & Accounting Research (CSMAR). Wharton University of Pennsylvania. https://wrds-www.wharton.upenn.edu/pages/about/data-vendors/china-stock-market-accounting-research-csmar/

Dalal S, Seth B, Radulescu M, Secara C, Tolea C (2022) Predicting fraud in financial payment services through optimized hyper-parameter-tuned XGBoost model. Mathematics 10(24):4679. https://doi.org/10.3390/math10244679

Dantas RM, Firdaus R, Jaleel F, Neves Mata P, Mata MN, Li G (2022) Systemic acquired critique of credit card deception exposure through machine learning. J Open Innov: Technol Mark Complex 8(4):192. https://doi.org/10.3390/joitmc8040192

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

Domashova J, Kripak E (2022) Development of a generalized algorithm for identifying atypical bank transactions using machine learning methods. Procedia Comput Sci 213:101–109. https://doi.org/10.1016/j.procs.2022.11.044

Dutta I, Dutta S, Raahemi B (2017) Detecting financial restatements using data mining techniques. Expert Syst Appl 90:374–393. https://doi.org/10.1016/j.eswa.2017.08.030

Elshaar S, Sadaoui S (2020) Semi-supervised Classification of Fraud Data in Commercial Auctions. Appl Artif Intell 34(1):47–63. https://doi.org/10.1080/08839514.2019.1691341

Esenogho E, Mienye ID, Swart TG, Aruleba K, Obaido G (2022) A neural network ensemble with feature engineering for improved credit card fraud detection. IEEE Access 10:16400–16407. https://doi.org/10.1109/ACCESS.2022.3148298

Eshghi A, Kargari M (2019) Introducing a new method for the fusion of fraud evidence in banking transactions with regards to uncertainty. Expert Syst Appl 121:382–392. https://doi.org/10.1016/j.eswa.2018.11.039

Estupiñán Gaitán R (2015) Control interno y fraudes: análisis de informe COSO I, II y III con base en los ciclos transaccionales, Tercera edición (Niebel BW (ed)). Ecoe Ediciones

Fanai H, Abbasimehr H (2023) A novel combined approach based on deep autoencoder and deep classifiers for credit card fraud detection. Expert Syst Appl 217:119562. https://doi.org/10.1016/j.eswa.2023.119562

Fang Y, Zhang Y, Huang C (2019) Credit card fraud detection based on machine learning. Comput Mater Contin 61(1):185–195. https://doi.org/10.32604/cmc.2019.06144

Femila Roseline J, Naidu G, Samuthira Pandi V, Alamelu alias Rajasree S, Mageswari N (2022) Autonomous credit card fraud detection using machine learning approach☆. Comput Electr Eng 102:108132. https://doi.org/10.1016/j.compeleceng.2022.108132

García-Ordás MT, Alaiz-Moretón H, Casteleiro-Roca J-L, Jove E, Benítez-Andrades JA, García-Rodríguez I, Quintián H, Calvo-Rolle JL (2023) Clustering techniques selection for a hybrid regression model: a case study based on a solar thermal system. Cybern Syst 54(3):286–305. https://doi.org/10.1080/01969722.2022.2030006

Gupta S, Mehta SK (2021) Data mining-based financial statement fraud detection: systematic literature review and meta-analysis to estimate data sample mapping of fraudulent companies against non-fraudulent companies. Global Bus Rev https://doi.org/10.1177/0972150920984857

Hajek P, Henriques R (2017) Mining corporate annual reports for intelligent detection of financial statement fraud—a comparative study of machine learning methods. Knowl-Based Syst 128:139–152. https://doi.org/10.1016/j.knosys.2017.05.001

Hamza C, Lylia A, Nadine C, Nicolas C (2023) Semi-supervised method to detect fraudulent transactions and identify fraud types while minimizing mounting costs. Int J Adv Comput Sci Appl 14(2). https://doi.org/10.14569/IJACSA.2023.0140298

Hilal W, Gadsden SA, Yawney J (2022) Financial fraud: a review of anomaly detection techniques and recent advances. Expert Syst Appl 193:116429. https://doi.org/10.1016/j.eswa.2021.116429

Hofmann H (1994) Statlog (German credit data). UCI Machine Learning Repository. https://doi.org/10.24432/C5NC77

Huang D, Mu D, Yang L, Cai X (2018) CoDetect: financial fraud detection with anomaly feature detection. IEEE Access 6:19161–19174. https://doi.org/10.1109/ACCESS.2018.2816564

Hwang J, Kim K (2020) An efficient domain-adaptation method using GAN for fraud detection. Int J Adv Comput Sci Appl 11(11). https://doi.org/10.14569/IJACSA.2020.0111113

Ileberi E, Sun Y, Wang Z (2021) Performance evaluation of machine learning methods for credit card fraud detection using SMOTE and AdaBoost. IEEE Access 9:165286–165294. https://doi.org/10.1109/ACCESS.2021.3134330

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

Khan S, Alourani A, Mishra B, Ali A, Kamal M (2022) Developing a credit card fraud detection model using machine learning approaches. Int J Adv Comput Sci Appl 13(3). https://doi.org/10.14569/IJACSA.2022.0130350

Kim J, Kim H-J, Kim H (2019) Fraud detection for job placement using hierarchical clusters-based deep neural networks. Appl Intell 49(8):2842–2861. https://doi.org/10.1007/s10489-019-01419-2

Kim YJ, Baik B, Cho S (2016) Detecting financial misstatements with fraud intention using multi-class cost-sensitive learning. Expert Syst Appl 62:32–43. https://doi.org/10.1016/j.eswa.2016.06.016

Kitchenham B, Brereton P (2013) A systematic review of systematic review process research in software engineering. Inf Softw Technol 55(12):2049–2075. https://doi.org/10.1016/j.infsof.2013.07.010

Kitchenham B, Stuart C (2007) Guidelines for performing systematic literature reviews in software engineering. https://www.researchgate.net/publication/302924724_Guidelines_for_performing_Systematic_Literature_Reviews_in_Software_Engineering

Kootanaee AJ, Aghajan AAP, Shirvani MH (2021) A hybrid model based on machine learning and genetic algorithm for detecting fraud in financial statements. J Optim Ind Eng 14(2):183–201. https://doi.org/10.22094/JOIE.2020.1877455.1685

KPMG (2022) Una triple amenaza en las Américas. KMPG. https://kpmg.com/co/es/home/insights/2022/01/kpmg-fraud-outlook-survey.html

Kumar S, Ahmed R, Bharany S, Shuaib M, Ahmad T, Tag Eldin E, Rehman AU, Shafiq M (2022) Exploitation of machine learning algorithms for detecting financial crimes based on customers' behavior. Sustainability 14(21):13875. https://doi.org/10.3390/su142113875

Kumbure MM, Lohrmann C, Luukka P, Porras J (2022) Machine learning techniques and data for stock market forecasting: a literature review. Expert Syst Appl 197:116659. https://doi.org/10.1016/j.eswa.2022.116659

Lee H, Choi E, Kim I, Choi D, Go W, Lee K, Yim H, Lee T (2018) Feature selection practice for unsupervised learning of credit card fraud detection. J Theor Appl Inf Technol 96(2):408–417

Lei X, Mohamad UH, Sarlan A, Shutaywi M, Daradkeh YI, Mohammed HO (2022) Development of an intelligent information system for financial analysis depend on supervised machine learning algorithms. Inf Process Manag 59(5):103036. https://doi.org/10.1016/j.ipm.2022.103036

Lokanan M, Tran V, Vuong NH (2019) Detecting anomalies in financial statements using machine learning algorithm. Asian J Account Res 4(2):181–201. https://doi.org/10.1108/AJAR-09-2018-0032

Lokanan ME, Sharma K (2022) Fraud prediction using machine learning: The case of investment advisors in Canada. Mach Learn Appl 8:100269. https://doi.org/10.1016/j.mlwa.2022.100269

Lokanan ME (2022) Predicting money laundering using machine learning and artificial neural networks algorithms in banks. J Appl Secur Res 1–25. https://doi.org/10.1080/19361610.2022.2114744

López-Rojas E (2017) Synthetic financial datasets for fraud detection. Kaggle. https://www.kaggle.com/datasets/ealaxi/paysim1

Machine Learning Group (2018) Credit card fraud detection. Kaggle. https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud

Madhurya MJ, Gururaj HL, Soundarya BC, Vidyashree KP, Rajendra AB (2022) Exploratory analysis of credit card fraud detection using machine learning techniques. Glob Transit Proc 3(1):31–37. https://doi.org/10.1016/j.gltp.2022.04.006

Malik EF, Khaw KW, Belaton B, Wong WP, Chew X (2022) Credit card fraud detection using a new hybrid machine learning architecture. Mathematics 10(9):1480. https://doi.org/10.3390/math10091480

Márquez Arcila RH (2019) Auditoría forense. Ecoe Ediciones

Misra S, Thakur S, Ghosh M, Saha SK (2020) An autoencoder based model for detecting fraudulent credit card transaction. Procedia Comput Sci 167:254–262. https://doi.org/10.1016/j.procs.2020.03.219

Moher D, Liberati A, Tetzlaff J, Altman DG (2009) Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. PLoS Med 6(7):e1000097. https://doi.org/10.1371/journal.pmed.1000097

Mongwe W, Malan K (2020) A survey of automated financial statement fraud detection with relevance to the South African context. S Afr Comput J 32(1). https://doi.org/10.18489/sacj.v32i1.777

Montes Salazar CA (2019) Riesgos de fraude en una auditoría de estados financieros (1.a ed.). Alfaomega. ISBN: 9789587782639. https://www.alfaomegacloud.com/reader/riesgos-de-fraude-en-una-auditoria-de-estados-financieros?location=3

Moreira MÂL, Junior C, de SR, Silva DF, de L, de Castro Junior MAP, Costa IP, de A, Gomes CFS, dos Santos M (2022) Exploratory analysis and implementation of machine learning techniques for predictive assessment of fraud in banking systems. Procedia Comput Sci 214:117–124. https://doi.org/10.1016/j.procs.2022.11.156

Narsimha B, Raghavendran CV, Rajyalakshmi P, Reddy GK, Bhargavi M, Naresh P (2022) Cyber defense in the age of artificial intelligence and machine learning for financial fraud detection application. Int J Electr Electron Res 10(2):87–92. https://doi.org/10.37391/ijeer.100206

Nian K, Zhang H, Tayal A, Coleman T, Li Y (2016) Auto insurance fraud detection using unsupervised spectral ranking for anomaly. J Financ Data Sci 2(1):58–75. https://doi.org/10.1016/j.jfds.2016.03.001

Nicholls J, Kuppa A, Le-Khac N-A (2021) Financial cybercrime: a comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. IEEE Access 9:163965–163986. https://doi.org/10.1109/ACCESS.2021.3134076

Nonnenmacher J, Marx Gómez J (2021) Unsupervised anomaly detection for internal auditing: Literature review and research agenda. Int J Digit Account Res 1–22. https://doi.org/10.4192/1577-8517-v21_1

Olszewski D (2014) Fraud detection using self-organizing map visualizing the user profiles. Knowl Based Syst 70:324–334. https://doi.org/10.1016/j.knosys.2014.07.008

Omershafiq (2019) Bitcoin network transactional metadata. Kaggle. https://www.kaggle.com/datasets/omershafiq/bitcoin-network-transactional-metadata

Ounacer S, Ait El Bour H, Oubrahim Y, Ghoumari MY, Azzouazi M (2018) Using isolation forest in anomaly detection: the case of credit card transactions. Period Eng Nat Sci 6(2):394. https://doi.org/10.21533/pen.v6i2.533

Palacio SM (2019) Abnormal pattern prediction: detecting fraudulent insurance property claims with semi-supervised machine-learning. Data Sci J 18(1):35. https://doi.org/10.5334/dsj-2019-035

Papík M, Papíková L (2022) Detecting accounting fraud in companies reporting under US GAAP through data mining. Int J Account Inf Syst 45:100559. https://doi.org/10.1016/j.accinf.2022.100559

Plakandaras V, Gogas P, Papadimitriou T, Tsamardinos I (2022) Credit card fraud detection with automated machine learning systems. Appl Artif Intell 36(1). https://doi.org/10.1080/08839514.2022.2086354

Polak P, Nelischer C, Guo H, Robertson DC (2020) Intelligent” finance and treasury management: what we can expect. AI Soc 35(3):715–726. https://doi.org/10.1007/s00146-019-00919-6

PricewaterhouseCoopers (2022) Encuesta Global de Crimen y Fraude Económico de PwC Colombia 2022–2023. https://www.pwc.com/co/es/publicaciones/encuesta-crimen-fraude-economico.html

Pumsirirat A, Yan L (2018) Credit card fraud detection using deep learning based on auto-encoder and restricted Boltzmann machine. Int J Adv Comput Sci Appl 9(1). https://doi.org/10.14569/IJACSA.2018.090103

Putten P (2000) Insurance Company Benchmark (COIL 2000). UCI Machine Learning Repository. https://doi.org/10.24432/C5630S

Quinlan R (1997) Statlog (Australian credit approval). UCI Machine Learning Repository. https://doi.org/10.24432/C59012

Rakowski R, Polak P, Kowalikova P (2021) Ethical aspects of the impact of AI: the status of humans in the era of artificial intelligence. Society 58(3):196–203. https://doi.org/10.1007/s12115-021-00586-8

Ramírez-Alpízar A, Jenkins M, Martínez A, Quesada-López C (2020a) Use of data mining and machine learning techniques for fraud detection in financial statements: a systematic mapping study. Rev Ibér Sist Tecnol Inf Lousada No. E28:97–109

Reurink A (2018) Financial fraud: a literature review. J Econ Surv 32(5):1292–1325. https://doi.org/10.1111/joes.12294

Rocha-Salazar J-J, Segovia-Vargas M-J, Camacho-Miñano M-M (2021) Money laundering and terrorism financing detection using neural networks and an abnormality indicator. Expert Syst Appl 169:114470. https://doi.org/10.1016/j.eswa.2020.114470

Roehrs A, da Costa CA, Righi R, da R, de Oliveira KSF (2017) Personal health records: a systematic literature review. J Med Internet Res 19(1):e13. https://doi.org/10.2196/jmir.5876

Rubio J, Barucca P, Gage G, Arroyo J, Morales-Resendiz R (2020) Classifying payment patterns with artificial neural networks: an autoencoder approach. Lat Am J Cent Bank 1(1–4):100013. https://doi.org/10.1016/j.latcb.2020.100013

Sahin Y, Bulkan S, Duman E (2013) A cost-sensitive decision tree approach for fraud detection. Expert Syst Appl 40(15):5916–5923. https://doi.org/10.1016/j.eswa.2013.05.021

Saputra M, Santosa PI, Permanasari AE (2023) Consumer behaviour and acceptance in fintech adoption: a systematic literature review. Acta Inform Pragensia 12(2):468–489. https://doi.org/10.18267/j.aip.222

Saragih MG, Chin J, Setyawasih R, Nguyen PT, Shankar K (2019) Machine learning methods for analysis fraud credit card transaction. Int J Eng Adv Technol 8(6S):870–874. https://doi.org/10.35940/ijeat.F1164.0886S19

Sathya M, Balakumar B (2022) Insurance fraud detection using novel machine learning technique. Int J Intell Syst Appl Eng 10(3):374–381

Savić M, Atanasijević J, Jakovetić D, Krejić N (2022) Tax evasion risk management using a hybrid unsupervised outlier detection method. Expert Syst Appl 193:116409. https://doi.org/10.1016/j.eswa.2021.116409

Seera M, Lim CP, Kumar A, Dhamotharan L, Tan KH (2021) An intelligent payment card fraud detection system. Ann Oper Res. https://doi.org/10.1007/s10479-021-04149-2

Shahana T, Lavanya V, Bhat AR (2023) State of the art in financial statement fraud detection: a systematic review. Technol Forecast Soc Change 192:122527. https://doi.org/10.1016/j.techfore.2023.122527

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

Singh A, Jain A, Biable SE (2022) Financial fraud detection approach based on firefly optimization algorithm and support vector machine. Appl Comput Intell Soft Comput 2022:1–10. https://doi.org/10.1155/2022/1468015

Smith Q-J, Valverde R (2021) A perceptron based neural network data analytics architecture for the detection of fraud in credit card transactions in financial legacy systems. WSEAS Trans Syst Control 16:358–374. https://doi.org/10.37394/23203.2021.16.31

Sofy MA, Khafagy MH, Badry RM (2023) An intelligent Arabic model for recruitment fraud detection using machine learning. J Adv Informat Technol. https://doi.org/10.12720/jait.14.1.102-111

Srokosz M, Bobyk A, Ksiezopolski B, Wydra M (2023) Machine-learning-based scoring system for antifraud CISIRTs in banking environment. Electronics 12(1):251. https://doi.org/10.3390/electronics12010251

Subudhi S, Panigrahi S (2020) Use of optimized fuzzy *C*-Means clustering and supervised classifiers for automobile insurance fraud detection. J King Saud Univ — Comput Inf Sci 32(5):568–575. https://doi.org/10.1016/j.jksuci.2017.09.010

Ti Y-W, Hsin Y-Y, Dai T-S, Huang M-C, Liu L-C (2022) Feature generation and contribution comparison for electronic fraud detection. Sci Rep 12(1):18042. https://doi.org/10.1038/s41598-022-22130-2

Tingfei H, Guangquan C, Kuihua H (2020) Using variational auto encoding in credit card fraud detection. IEEE Access 8:149841–149853. https://doi.org/10.1109/ACCESS.2020.3015600

Torrano C, Recuero P, Ramirez F, Hernández S, Torres J (2018) Machine learning aplicado a la ciberseguridad: técnicas y ejemplos en detección de amenazas. Zeroxword Computing

Udeze CL, Eteng IE, Ibor AE (2022) Application of machine learning and resampling techniques to credit card fraud detection. J Niger Soc Phys Sci 769. https://doi.org/10.46481/jnsps.2022.769

Usman A, Naveed N, Munawar S (2023) Intelligent anti-money laundering fraud control using graph-based machine learning model for the financial domain. J Cases Inf Technol 25(1):1–20. https://doi.org/10.4018/JCIT.316665

Van Capelleveen G, Poel M, Mueller RM, Thornton D, Van Hillegersberg J (2016) Outlier detection in healthcare fraud: a case study in the Medicaid dental domain. Int J Account Inf Syst 21:18–31. https://doi.org/10.1016/j.accinf.2016.04.001

Vanhoeyveld J, Martens D, Peeters B (2020) Value-added tax fraud detection with scalable anomaly detection techniques. Appl Soft Comput 86:105895. https://doi.org/10.1016/j.asoc.2019.105895

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

Vanneschi L, Horn DM, Castelli M, Popovič A (2018) An artificial intelligence system for predicting customer default in e-commerce. Expert Syst Appl 104:1–21. https://doi.org/10.1016/j.eswa.2018.03.025

Viera J, Aguilar J, Rodríguez-Moreno M, Quintero-Gull C (2023) Analysis of the behavior pattern of energy consumption through online clustering techniques. Energies 16(4):1649. https://doi.org/10.3390/en16041649

Wadhwa VK, Saini AK, Kumar SS (2020) Financial fraud prediction models: a review of research evidence. Int J Sci Technol Res 9(1):677–680

West J, Bhattacharya M (2016) Intelligent financial fraud detection: a comprehensive review. Comput Secur 57:47–66. https://doi.org/10.1016/j.cose.2015.09.005

Whiting DG, Hansen JV, McDonald JB, Albrecht C, Albrecht WS (2012) Machine learning methods for detecting patterns of management fraud. Comput Intell 28(4):505–527. https://doi.org/10.1111/j.1467-8640.2012.00425.x

Wohlin C (2014) Guidelines for snowballing in systematic literature studies and a replication in software engineering. In: Proceedings of the 18th international conference on evaluation and assessment in software engineering. pp. 1–10

Wu B, Lv X, Alghamdi A, Abosaq H, Alrizq M (2023) Advancement of management information system for discovering fraud in master card based intelligent supervised machine learning and deep learning during SARS-CoV2. Inf Process Manag 60(2):103231. https://doi.org/10.1016/j.ipm.2022.103231

Xiong T, Ma Z, Li Z, Dai J (2022) The analysis of influence mechanism for internet financial fraud identification and user behavior based on machine learning approaches. Int J Syst Assur Eng Manag 13(S3):996–1007. https://doi.org/10.1007/s13198-021-01181-0

Xiuguo W, Shengyong D (2022) An analysis on financial statement fraud detection for Chinese listed companies using deep learning. IEEE Access 10:22516–22532. https://doi.org/10.1109/ACCESS.2022.3153478

Yeh I-C (2016) Default of credit card clients. UCI Machine Learning Repository. https://doi.org/10.24432/C55S3H

Zhang Z, Zhou X, Zhang X, Wang L, Wang P (2018) A model based on convolutional neural network for online transaction fraud detection. Secur Commun. Netw. 2018:1–9. https://doi.org/10.1155/2018/5680264

Zhao Z, Bai T (2022) Financial fraud detection and prediction in listed companies using SMOTE and machine learning algorithms. Entropy 24(8):1157. https://doi.org/10.3390/e24081157

Zhou H, Chai H, Qiu M (2018) Fraud detection within bankcard enrollment on mobile device based payment using machine learning. Front Inf Technol Electron Eng 19(12):1537–1545. https://doi.org/10.1631/FITEE.1800580

Zupan M, Budimir V, Letinic S (2020) Journal entry anomaly detection model. Intell Syst Account Financ Manag 27(4):197–209. https://doi.org/10.1002/isaf.1485

Acknowledgements

We would like to express our gratitude to the Universidad Cooperativa de Colombia, Ibagué campus, Espinal. This research work was supported by Universidad Cooperativa de Colombia and derived from research project INV3456 entitled "Detection of anomalies in financial data in social economy organizations through machine learning techniques" associated with the PLANAUDI, AQUA and SINERGIA UCC group, from the Research Center of the Public Accounting and Systems Engineering program of the UCC Ibagué campus.

Author contributions

All authors contributed to the creation and design of the study.

Competing interests

The authors declare no competing interests.

Ethical approval and consent to participate

The authors declare that they have no human participants, human data, or human tissue.

Consent to publish

The authors have no data from any individual person on any form.

Additional information

Correspondence and requests for materials should be addressed to Ludivia Hernandez Aros.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Open Access This article is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License, which permits any non-commercial use, sharing, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if you modified the licensed material. You do not have permission under this licence to share adapted material derived from this article or parts of it. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by-nc-nd/4.0/.

© The Author(s) 2024