Research Article

Artificial Intelligence Driven Approaches for Financial Fraud Detection: A Systematic Literature Review

Indrawati Yuhertiana and Ahsanul Hadi Amin*

Faculty of Economics and Business, Universitas Pembangunan Veteran Jawa Timur, Surabaya, Indonesia

Abstract.
The primary aim of this research is to present a thorough and all-encompassing examination of artificial intelligence (AI) methodologies employed in the detection of financial fraud. The present study employs a systematic literature review (SLR) that was conducted utilizing the PRISMA approach. A comprehensive search was undertaken on reputable academic databases including ScienceDirect, Scopus, Springer, and Emerald, yielding a total of 24 papers published throughout the timeframe of 2014 to 2023. These articles will, thereafter, undergo further analysis. The findings of this study demonstrate that the implementation of artificial intelligence (AI) techniques for detecting financial fraud yields favorable outcomes. Specifically, the AI approach proves to be effective in enhancing the precision and efficiency of fraud pattern identification, thereby making a substantial contribution in this domain. In contrast, the prevailing methodology employed in the realm of financial fraud detection is frequently centered around machine learning. Furthermore, a majority of the research encompassed a diverse range of industries, with particular emphasis on the financial industry as the primary domain for the implementation of artificial intelligence (AI) in the detection of financial fraud.

Keywords: artificial intelligent, financial fraud, fraud detection

Corresponding Author: Ahsanul Hadi Amin; email: 22062020001@student.upnjatim.ac.id

Published: 4 July 2024

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the 3rd JESICA Conference Committee.

1. Introduction

Fraud, a term commonly referred to as fraudulent activities, continues to be a compelling and significant subject for exploration and investigation in the numerous instances that persist in contemporary society. Fraud, as defined by the Association of Certified Fraud Examiners (ACFE), encompasses the intentional exploitation of one's position for personal gain by means of misusing an organization's assets or resources. According to Sudarmanto [1], in recent times, there has been a notable rise in occurrences of financial fraud, which has had detrimental effects on the trust and credibility among corporations, regulatory bodies, and participants in the market. Moreover, this surge in fraudulent activities poses a significant risk to the entire functioning and efficacy of financial markets [2]. Within the context of a progressively intricate corporate landscape, individuals engaging in fraudulent activities employ progressively advanced strategies, including

How to cite this article: Indrawati Yuhertiana and Ahsanul Hadi Amin*, (2024), "Artificial Intelligence Driven Approaches for Financial Fraud Detection: A Systematic Literature Review " in *The 3rd Jakarta Economic Sustainability International Conference*, KnE Social Sciences, pages 448–468. DOI 10.18502/kss.v9i20.16551

the utilization of malware attacks and data manipulation techniques that are challenging to identify. According to Sun et al. [3], additionally, the integration of financial technology (fintech) and the advancement of digital financial systems have created opportunities for novel forms of fraudulent activities that can exploit vulnerabilities in security measures. The aforementioned factors have resulted in an elevated susceptibility and exposure to instances of financial fraud, thereby posing a significant risk to the stability and trustworthiness of the worldwide financial markets [4].

The vast magnitude of digital financial transactions and the substantial volume of associated data pose challenges for human operators in identifying abnormalities within the financial system and differentiating them from incidental or systematic errors that may not be directly linked to financial operations and goods [5]. Given the inherent limits of human beings, there is a desire to develop a system capable of effectively addressing anomalies within the financial domain, with the ultimate goal of establishing a state of reliable security and long-term viability [6]. In our contemporary society, characterized by a growing reliance on digital technologies and intricate systems, the significance of artificial intelligence (AI) in identifying anomalies and detecting fraudulent activities has emerged as a highly anticipated and indispensable aspect for organizations as a whole. Artificial intelligence (AI) has emerged as a significant force in assisting institutions, including companies and governments, in preserving data integrity and safeguarding against a range of fraudulent risks that pose potential harm [7]. Artificial intelligence (AI) possesses the capacity to evaluate vast amounts of data and identify patterns that may be deemed suspicious or unsuitable, owing to its continuously advancing intelligence. Artificial intelligence (AI) possesses the capability to monitor transactions and behavior in real-time, so enabling the prompt identification of potential fraudulent activities, even prior to their detrimental impact on the parties concerned [3].

The cognitive capabilities of artificial intelligence (AI) prove to be highly advantageous in detecting and thwarting fraudulent activities. In the context of mitigating fraudulent activities in financial reporting, an AI model is employed. This model leverages machine learning and artificial intelligence techniques to discern patterns linked to significant instances of financial fraud that exert a profound influence on the organization's standing. The model has a high level of efficacy in detecting instances of fraud, irrespective of the direct relevance of the observed information to the fraudulent action [8]. The utilization of artificial intelligence (AI) is anticipated to provide favorable outcomes for companies and entities, as it offers advantages in terms of enhancing viability and sustainability.

Artificial Intelligence (AI) has become extensively employed in the finance domain, encompassing banking, industry, and various other areas, during its evolutionary trajectory [9]. The utilization of artificial intelligence (AI) in the identification of fraudulent activities provides a novel approach for organizations, as it streamlines the process of fraud detection [6]. The usefulness of artificial intelligence (AI) technology in the realm of fraud detection will enhance the efficiency of professionals engaged in endeavors to mitigate and identify fraudulent behaviors. Routine duties such as the collection of transaction data, data processing, and analysis of potential fraudulent activities can become tedious and time-consuming when performed manually. Artificial intelligence (AI) enables fraud detection systems to rapidly and effectively scan and analyze vast and intricate transactional data, hence enhancing their ability to efficiently spot trends or indicators of fraudulent activity [10].

Numerous systematic literature reviews (SLRs) have been undertaken to investigate the application of artificial intelligence (AI) in fraud detection within the financial domain. Noteworthy studies in this area include the research conducted by Abedini et al. [7], Cherif et al. [11], Pinto and Sobreiro [5], and Sun et al. [3]. So far, scholarly investigations have primarily concentrated on the application of artificial intelligence (AI) in the realm of fraud detection, particularly within sectors such as banking, corporate, and capital markets. Hence, there exists a notable prospect to conduct more investigation pertaining to the integration of artificial intelligence (AI) with the aim of enhancing the detection of financial fraud in a more complete manner. Therefore, this literature analysis is anticipated to make a significant scholarly contribution by enhancing comprehension of the influence and utilization of artificial intelligence (AI) technology in the identification of financial fraud, a pervasive occurrence within diverse domains of business and finance.

The PICO technique is commonly employed by researchers for the purpose of creating research questions. The population (P) encompasses all entities that are subject to analysis under the specific research theme selected by the investigator. The term “intervention” (I) denotes the course of action that has to be implemented in order to effectively address the identified problem. The term “Comparison” (C) denotes an alternative action that can be employed for the purpose of comparison, while “Outcome” (O) pertains to the findings of prior studies that serve as the primary focus of the research [12].

There are three research questions, i.e.:

(a) Which industry or sector of business utilizes artificial intelligence for the purpose of detecting instances of financial fraud?

(b) What types of technology and algorithms pertaining to artificial intelligence are employed in the identification and prevention of financial fraud?

(c) To what extent does an AI-based strategy demonstrate efficacy in the detection of financial fraud?

2. Material and Methods

The approach utilized in this study is a systematic literature review (SLR) methodology. The utilization of literature reviews offers substantial advantages in the consolidation of diverse and pertinent study findings. By employing this approach, the material being presented attains a higher level of comprehensiveness and balance. The primary objective of a systematic literature review is to conduct a comprehensive investigation in a transparent manner, with the intention of including all published sources of information pertaining to a certain subject. Additionally, the study tries to assess the quality of the evidence presented in these sources [13]. According to the recommendations provided, this investigation comprises multiple sequential steps, as outlined by Page et al. [14]. In this section, we will explain the eligibility conditions and the various sources of knowledge. The selection of studies refers to choosing specific data items from a larger dataset for analysis or further processing. The data collection process involves systematically gathering information or data for research purposes. This includes identifying relevant variables, selecting appropriate data collection methods, and implementing these methods to collect data.

2.1. Eligibility criteria

The literature criteria encompass the inclusion and exclusion criteria, which have been altered to align with the PICO framework. The modifications made to the PICO framework include the following additions :

Table 1: Inclusion and Exclusion Criteria.

Criteria	**Inclusion**	**Exclusion**
Publish Period	2014-2023	Before 2014
Subject	Business, management and accounting, Economic, Econometrics and Finance, and Computer Science	Non articles relate with business, management, and accounting Econometrics and Finance, and Computer Science subject
Types of articles	Research articles	Non research articles
Keywords, Titles, Abstract	Keywords, titles and abstract focus on the application of AI in fraud detection in the financial sphere	Keywords, titles and abstracts do not focus on the application of AI in financial fraud detection
Screening articles	The selected article does match the context of the topic in this study	The selected article does not match the context of the topic in this study
Language	English	Non-English

Source: Author’s own work’

2.2. Information sources

The study conducted comprehensive searches across key online databases of reputable study repositories, including Sciendirect, Scopus, Springer, and Emerald. The study employed a rigorous selection process, focusing exclusively on publications that were readily available and have comprehensive documentation. This approach ensured that only articles meeting these criteria were included in the subsequent analysis. This measure was implemented in order to guarantee the highest possible standard and accessibility of information during the data gathering process, in conjunction with endeavors to locate scholarly literature from reputable and authoritative sources within the research field.

2.3. Study selection

The research selection process commenced by doing a comprehensive search of article databases utilizing various keywords including “Fraud,” “Fraud detection,” “Artificial Intelligence,” “AI,” “Machine Learning,” “Deep Learning,” and “Financial Fraud Detection.” The research conducted a search using various Boolean combinations of operators (AND, OR). These combinations included phrases such as “Fraud Detection” AND “AI”, “Fraud Detection” AND “Machine Learning”, “Fraud Detection” AND “Deep Learning”, “Financial Fraud” AND “AI”, “Financial Fraud” AND “Machine Learning”, “Financial Fraud” AND “Deep Learning”, “Fraud AND AI”, “Financial fraud” OR “Fraud”, “Fraud Detection” AND (Machine Learning OR “Deep Learning”).

The researchers conducted a comprehensive literature search using various academic databases, including Sciendirect, Scopus, Springer, and Emerald. They employed specific keywords to refine their search and applied the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta Analyses) method. This method involves three distinct stages that are determined by the inclusion and exclusion criteria outlined in Fig. 1.

2.4. The process of data collection

The process of data gathering in the chosen study involves reading the article and subsequently extracting specific information such as the title, year of publication, author(s), country of origin, research objectives, research methodologies employed, type or approximation of artificial intelligence utilized, sector or industry in which the AI was applied, and the resulting outcomes.

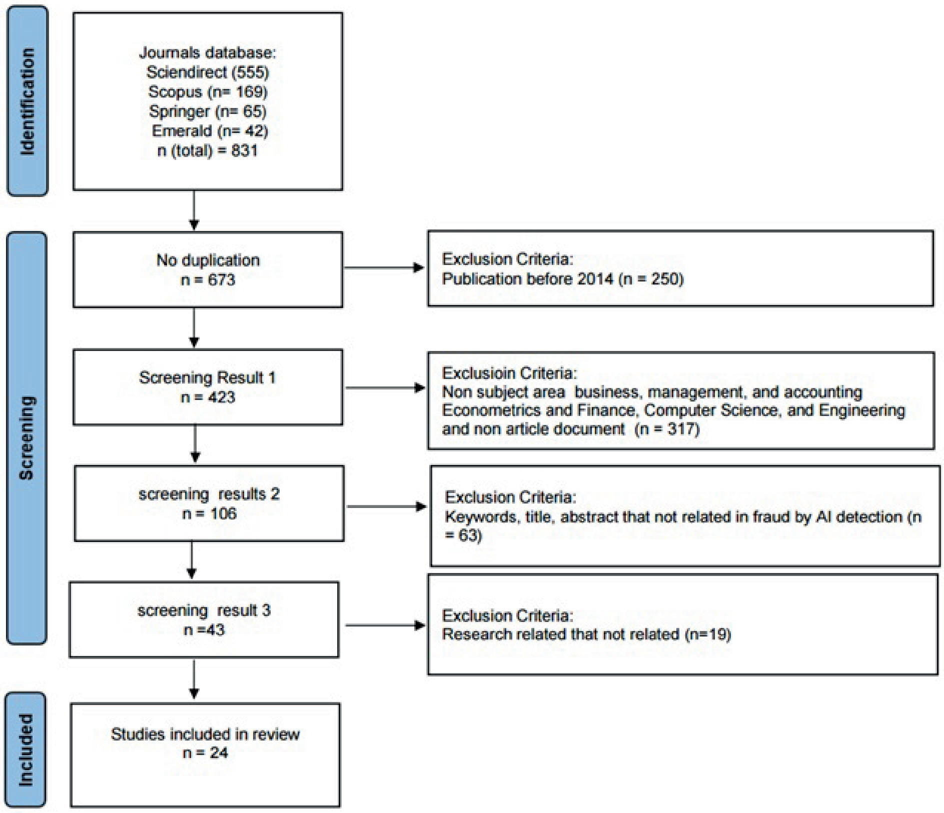
Identification
Journals database:
Sciendirect (555)
Scopus (n= 169)
Springer (n= 65)
Emerald (n= 42)
n (total) = 831
Screening
No duplication
n = 673
Exclusion Criteria:
Publication before 2014 (n = 250)
Screening Result 1
n = 423
Exclusioin Criteria:
Non subject area business, management, and accounting Econometrics and Finance, Computer Science, and Engineering and non article document (n = 317)
screening results 2
n = 106
Exclusion Criteria:
Keywords, title, abstract that not related in fraud by AI detection (n = 63)
screening result 3
n =43
Exclusion Criteria:
Research related that not related (n=19)
Included
Studies included in review
n = 24

Figure 1: PRISMA Flowchart (Source: Author's own work'.

2.5. The process of selecting data items.

The information derived from the aforementioned article encompasses the extent of the business or industry sector that use artificial intelligence in the identification of financial fraud. The utilization of artificial intelligence technologies and algorithms in the identification and detection of fraudulent activities within the realm of finance and the efficacy of artificial intelligence (AI) methods in the identification and prevention of financial fraud.

3. Results

3.1. Data selection results

The following is a table of the research/studies that we have collected through the selection process. Table 2 displays some of the key items in each of the selected studies in order to provide a detailed overview of the context of this research. In addition, this table provides and assists in exploring previous studies that is useful for obtaining information to fulfill the research question that has been previously set.

TABLE 2: Selection Results.

No	Title, Years	Authors, Country	Research Purpose	Research Method	Type AI, Industry Sector	Findings
1	Interpretable online banking fraud detection based on hierarchical Attention mechanism, 2019	Achituve et al. [9], Israel	To develop an attention-based architecture that can classify online banking transactions as fraudulent or genuine and additionally provide an interpretation of the results of such architecture	The study uses the experimental approach	Deep Learning, Banking industries	Research results show that the proposed attention-based architecture IS capable of providing accurate predictions for fraud classification on online banking transaction data. The results suggest that the attention mechanisms applied in the model have a significant influence on improved performance and interpretative ability of the client
2	Comparative analysis of credit card fraud detection in Simulated Annealing trained Artificial Neural Network and Hierarchical Temporal Memory, 2022	Osegi and Jumbo [15], Nigeria	The aim of this study is to discuss how machine learning methods classification algorithms can be used to predict fraud in financial transactions	This study uses the comparative method of Experimental	Deep Learning or Machine Learning, banking	The results of the study show that increasing the size of data samples can improve the accuracy of CCF detection with HTM-CLA. Although HTM CLA competes with conventional neural techniques that use Simulated Annealing (SA-ANN). This technique may not always provide the highest precision but has advantages in system design and resilience for applications in real-world CCF Detection environments as well as improving its detection in recognizing anomaly fraud
3	Detection of fraudulent transactions using SAS Viya machine learning algorithms, 2020	Domashova and Zabelina [16], Russia	The aim of this study was to test the relationship between power-building auditing and the Accounting Information System (AIS) in healthcare fraud audits conducted by the government in the United States	A quantitative research study	Machine Learning, Banking	The main finding of this study is that machine learning algorithms can effectively detect fraudulent transactions in the financial system

Table 2: Continued.

No	Title, Years	Authors, Country	Research Purpose	Research Method	Type AI, Industry Sector	Findings
4	Towards automated feature engineering for credit card fraud detection using multi- perspective HMMs, 2021	Lucas et al. [17], Germany	The main objective of this research IS to propose method to improve fraud detection in credit card transactions using historical-based features generated by Hidden Markov Models (HMM)	Experimental study	Machine Learning, Banking	The main finding of this study is that the proposed multiple-perspective-based approach of the Hidden Markov Model (H MM) turns out to outperform the existing technique in terms of accuracy and area below the ROC curve to detect fraudulent transaction. The study found that combining the proposed approach with existing techniques such as peer group analysis and descriptive statistics could result in further improvements in fraud detection
5	Chinese corporate fraud risk assessment with machine learning, 2023	Lu et al. [18], China	The main objective of this study is to introduce genuine corporate fraud detection model that utilizes machine learning techniques and open data sets of CSMAR	A quantitative research study	Machine Learning, Chinese stock market	The main finding of the study is that a machine-learning based fraud risk assessment model significantly improves the performance of company fraud Detection in China's stock market
6	Leveraging machine learning the global fight against money laundering and Terrorism financing: An affordances perspective, 2021	Canhoto [19], UK	The main purpose of this study is to explore the technical and contextual features of anti-money laundering (AML) profile development in UK-based financial services organization using case study approach	Case study	Machine learning Financial Services Organization or Bank	The findings of this study suggest that the use of AI can help financial institutions in identifying patterns of behavior followed by customers to hide the source or use of illegal money
7	Intelligent financial fraud detection practices post-pandemic era, 2020	Zhu et al. [20], China	The objective of this study is to explore various types of fraud in the financial sector and to test the effectiveness of different methods in detecting and preventing fraudulent activities	Surveys	Machine Learning, financial sector industries	The utilization of surveys in the context of machine learning within the financial sector companies. However, the performance of the detection method relies on the quality and quantity of the data utilized. Moreover this study also demonstrates that the effectiveness of fraud detection can be enhanced by integrating different approaches and methods

Table 2: Continued.

No	Title, Years	Authors, Country	Research Purpose	Research Method	Type AI, Industry Sector	Findings
8	Exploratory analysis and implementation of machine learning techniques for predictive assessment of fraud in banking systems, 2022	Moreira et al. [21], Brazil	To analyze the application of machine learning algorithms for predictive assessment of fraud detection in banking systems	Experimental study (A quantitative research study)	Machine Learning, Banking	This study presents the key validity of each model in each scenario, which can help predict fraud in the banking system effectively
9	Fraud prediction using machine learning: The case of investment advisors in Canada, 2022	Lokanan and Sharma [22], Canada	The aim of this research to improve the detection of fraud using machine learning, especially in one of the domains where fraud detection is considered an important issue	A quantitative study that utilizes data gathering from IIROC enforcement cases between 2008 and 2019	Machine Learning, Canada's financial markets	The key findings of this study are that advanced machine learning algorithms, Random Forest Classifier (RFC), can accurately predict fraud in the financial market. This study is the first to use a machine learning model to test the symptoms of fraud and explore specific variables related to financial market regulation
10	On the Benefits of Machine Learning Classification in Cashback Fraud Detection, 2022	Karunachandi et al. [23], Indonesia	The main purpose of this research is to detect cashback fraud on e- commerce transactions	Experimental research	Machine Learning, E Commerce	The main findings of this study are the k-Nearest Neighbor (k-NN) algorithm combined with outlier detection methods resulting in an optimal rate of fraud detection with reduction in the level of false alarms
11	Refined analysis and a hierarchical multi-task learning approach for loan fraud detection, 2023	Chen et al. [24], China	The main objective of this study is to propose new deep learning- based framework namely hybrid multi-task learning (HMTL)	Experimental research	Deep Learning, the automobile finance sector	to detect car loan fraud by identifying various types of false information
12	Credit Fraud Detection Based on Hybrid Credit Scoring Model, 2023	Chen et al. [25], China	The primary objective of this study is to develop hybrid credit rating model that combines logistical regression and weighted evidence to improve the accuracy of credit ratings and reduce the incidence of credit fraud	Computational research study	Machine Learning, Banks and other financial institutions	The use of AI techniques in this research is critical to the detection and detection of fraud. The study uses in-depth learning techniques to develop models that detect trading anomalies common to fraudulent activities

TABLE 2: Continued.

No	Title, Years	Authors, Country	Research Purpose	Research Method	Type AI, Industry Sector	Findings
13	Using GNN to detect financial fraud based on the related party transactions network, 2022	Mao et al. [26], China	The main objective of this study was to use a graphic neural network to detect financial fraud based on a party -related transaction network Empirical (Quantitative) Graph neural networks (Machine learning), Companies in the financial sector	Computational research study	Machine Learning, Banks and other financial institutions	The authors found that adding KPT information to traditional financial indicators can significantly improve the accuracy of fraud detection ,and their GNN -based approach achieves the highest accuration and AUC
14	An Autoencoder Based Model for Detecting Fraudulent Credit Card Transaction, 2020	Misra et al. [27], India	The primary objective of this study is to propose a two -stage model to identify credit card fraud	Experimental	Machine learning, Ranking	This study highlights the correlation between AI and fraud detection, as the study proposes a model that uses machine learning techniques to detect fraud. The autoencoder is used to extract relevant features from the data, which are then classified as false or valid
15	Comparison of Poison process and machine leaming algorithms approach for credit card fraud detection, 2021	Izotova and Valiullin [28], Russia	The main objective of this study is to compare different approaches to detect credit card fraud	Study case	Machine learning. financial sector	The study found that the best results were obtained using gradient enhancement algorithms
16	Fraud Detection in Enterprise Resource Planning Systems using One-Class Support Vector Machine Combined with Convolutional Neural Network: The Case of Spor Istanbul, 2023	Arslan and Güneş [29], Turkey	The main objective of this research is to propose a new approach to performing anomaly detection in an Enterprise Resource Planning (ERP) 0system using machine learning algorithm	Experimental (quantitative)	Machine learning. sports enterprise	This approach is effective in detecting, potential security threats and system errors and can help organizations increase their chances of success by addressing essential elements of successful ERP implementation
17	Detection of fraudulent financial statements using the hybrid data mining approach, 2016	Chen [30], Taiwan	The purpose of this research is to develop a reliable and accurate model for detecting fraudulent financial reports	Experimental	Machine learning, company that experiences both fraudulent and non-fraudulent financial	Based on the empirical results of this research, the accuracy of DT CHAID combined with CART in detecting financial statement fraud is relatively high

TABLE 2: Continued.

No	Title, Years	Authors, Country	Research Purpose	Research Method	Type AI, Industry Sector	Findings
18	A machine leaming based credit card fraud detection using the GA algorithm for feature Selection, 2022	Lleberi et al. [32], South Africa	This study proposes a credit -based machine learning (Ml) approach, a fraud detection machine for credit cards using genetic algorithms (GA)for feature selection	Experimental	Machine Learning, bank	RF method was found to have the highest accuracy in detecting fraud for most of the tested feature vectors, with v5 achieving the best overall results
19	E-Commerce Fraud Detection Model by Computer Artificial Intelligence Data Mining, 2022	Li [33], China	This research aims to identify e-commerce fraud using AI	Experimental	computer artificial intelligence data mining, E-Commerce	The main finding of this research is that although the use of data mining techniques and machine learning algorithms insists in detecting fraud in e-commerce, effective verification of model accuracy and identification of fraudulent users in all aspects of technology are still necessary
20	Detecting anomalies in Financial statements using machine learning algorithm, 2019	Lokanan et al. [33], Vietnam	The aim of this study is to evaluate the possibility of assessing the creditworthiness rating of quarterly financial statements of a company using dynamic anomaly detection methods	Empirical studies	Machine Learning, Vietnamese listed firms	The findings indicate that the model is capable of rating quarterly financial statements based on creditworthiness. Executing the model on all observations also revealed that the majority of financial statements from companies listed on the stock exchange in Vietnam are trustworthy, but nearly a quarter of these companies are highly suspicious and warrant questioning
21	Predictive Modelling for Credit Card Fraud Detection Using Data Analytics, 2018	Patil et al. [34], India	The main objective of this research is to propose a real-time fraud detection system in financial transactions using analytical models such as logistic regression and decision tree machine learning models	Experimental	Machine Learning. Bank	The main finding of this research is that the logistic regression model developed in the study can accurately predict financial transaction fraud, achieving a high classification accuracy of 92.6%. This indicates that the proposed system can be an effective solution for real-time fraud detection in financial transactions

TABLE 2: Continued.

No	Title, Years	Authors, Country	Research Purpose	Research Method	Type AI, Industry Sector	Findings
22	A novel model for credit card fraud detection using Artificial Immune Systems, 2014	Halvaiee and Akbar [35], Iran	The primary objective of this research is to address the issue of credit card fraud detection by developing an Artificial Immune Recognition System (AIRS) to enhance fraud detection capabilities	Experimental	Artificial Immune System, bank	The study indicates that the AFDM algorithm is capable of detecting fraud with high accuracy, low computational cost, and minimal false positives
23	Detecting the financial statement fraud: The analysis of the differences between data mining techniques and experts' judgments, 2015	Lin et al. [36], Taiwan	The objective of this research is to examine all aspects of the fraud triangle by utilizing data mining techniques and using available and public information as proxy variables to evaluate attributes such as pressure incentive opportunity, and attitude/rationalization	Experimental	Data Mining, Securities company	This study demonstrates that neural network systems are valuable tools for practitioners in identifying fraud risks, and investing in this method can help prevent detrimental fraud within organization
24	Enhancement of fraud detection for narratives in annual reports, 2017	Chen et al. [37], Taiwan	The objective of this research is to create intelligent financial fraud detection by identifying fraudulent financial reporting	Experimental	machine learning, several companies in Taiwan	The results of this research indicate that machine learning classification algorithms can be effectively utilized to detect financial fraud in financial reporting

3.2. Business scope or business sector that uses AI to detect financial fraud

The utilization of artificial intelligence (AI) in various industrial sectors exhibits discernible variations in patterns that are of notable significance (Fig. 2). Within the realm of the financial sector, the use of artificial intelligence (AI) has the most prominent prevalence, accounting for a substantial proportion of 63%. The financial sector has emerged as the primary industry in adopting artificial intelligence (AI) technologies. Specifically, AI is being utilized to combat fraudulent activities in various business functions within this sector. For instance, AI is employed to identify and flag fraudulent anomalies in credit card usage [15, 17, 25, 28, 34, 35]. Additionally, AI is employed to detect fraudulent transactions in online banking [9], identify potential instances of money laundering [19], and implement predictive models to anticipate and prevent fraud [18, 21].

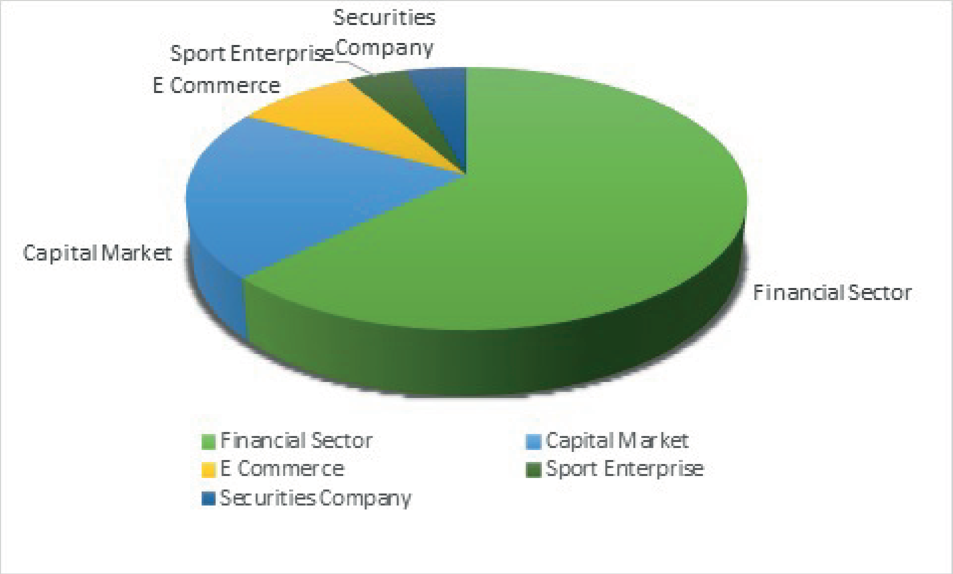

Figure 2: Pie Chart Application of AI in Fraud Detection in Several Sectors. (Source: Selection of previous studies).

In practical use, the capital market sector (comprising 21% of the market) leverages artificial intelligence (AI) technology to identify instances of fraudulent activities. The integration of artificial intelligence (AI) in capital markets serves two primary purposes: ensuring the sustainability of business operations and safeguarding against cyberattacks. AI technology plays a crucial role in mitigating fraudulent activities within the financial sector. Specifically, it is employed in assessing the risk of financial fraud through the application of risk-based assessment techniques [18, 22]. Additionally, AI is utilized for detecting instances of fraud in financial reporting [33, 37]. The utilization of artificial intelligence (AI) in the realm of e-commerce has been observed to encompass several applications, including the identification of anomalies and indicators of fraudulent activity. For instance, predictive models have been employed to detect AI-related irregularities, as well as to identify instances of cashback fraud [23]. Securities firms have been observed to employ artificial intelligence (AI) technology, specifically at a rate of 4 percent, for the purpose of fraud detection. This application of AI involves the identification and assessment of fraud risk inside investment activities [36]. In contrast, the sports business sector, comprising 4% of the sample, also expressed a desire to adopt artificial intelligence (AI) technology. Specifically, AI is utilized in the identification of fraudulent anomalies inside the enterprise resource planning (ERP) system. According to Arslan [29].

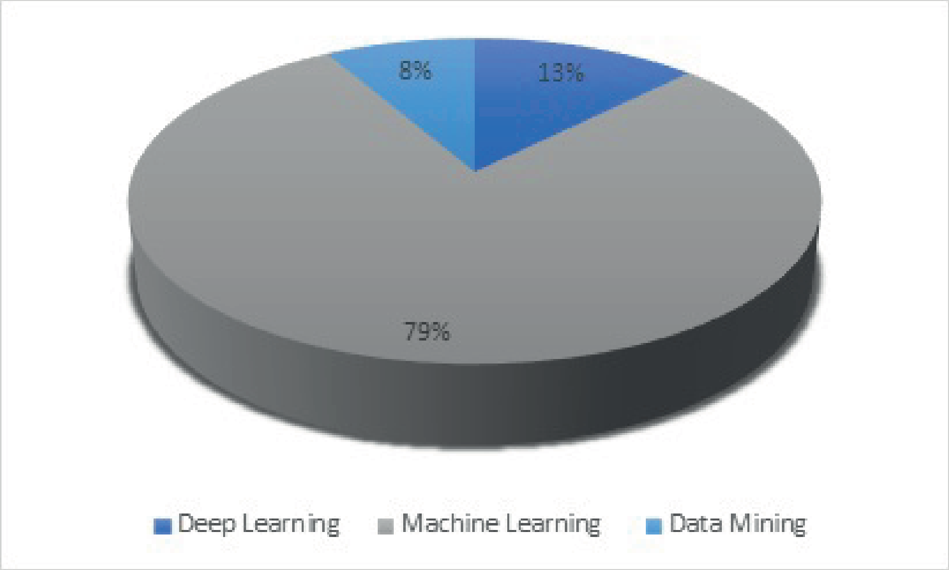

Figure 3: Pie Chart Technology and Artificial Intelligence Algorithms Used. (Source: Selection of previous studies).

3.3. Artificial intelligence technology and algorithms used in financial fraud detection

In the realm of AI-based financial fraud detection, Fig. 3 demonstrates that Deep Learning accounted for 8% of the contributions. This indicates that attention-based architectures [9], Artificial neural networks [15], and HTML approaches [18] have proven to be effective and productive in the domain of financial fraud detection. On the contrary, Machine Learning holds a significant majority share of 79%, indicating its predominant utilization in the implementation of predictive models [18, 19, 21, 23, 25, 28, 31, 33, 34, 35, 37]. Additionally, the HMM model [17], the RFC model [22], and the graphical neural network model are employed to detect anomalous patterns indicative of suspicious financial activity. Data mining has been found to provide a significant contribution of 13% in the field, underscoring its significance in extracting valuable insights from extensive and intricate datasets. These insights can then be utilized to inform and enhance decision-making processes related to fraud detection [2, 36].

3.4. The effectiveness of AI-driven approaches in detecting financial fraud

The efficacy of artificial intelligence (AI) based methodologies in the realm of Financial Fraud Detection The utilization of artificial intelligence (AI) in the identification of fraudulent activities, particularly within the financial domain including banking and other related establishments, has exhibited notable efficacy as indicated by the research findings presented in table 2. Several studies employ different forms of artificial intelligence (AI) to improve the effectiveness of fraud detection. For instance, researchers have utilized specialized techniques like Hidden Markov Models (HMM) [17] and Graph Neural Networks (GNN) [26] for this purpose. The results indicate that machine learning models applied in various industries such as finance, e-commerce, and securities demonstrate the capability of artificial intelligence (AI) to accurately classify anomalies and identify fraudulent financial activities [18, 19, 21, 23, 25, 28, 31, 33, 34, 35, 37].

Moreover, the application of deep learning has demonstrated favorable outcomes in detecting instances of financial fraud across the aforementioned domains. The aforementioned studies indicate that deep learning methods play a crucial role in enhancing the precision and effectiveness of identifying intricate and ever-changing patterns that traditional techniques may struggle to detect [9, 15, 24].

4. Discussion

Based on empirical evidence, it has been observed that the financial sector, encompassing banks and many other financial institutions, exhibits the highest degree of utilization of artificial intelligence techniques for the purpose of identifying and detecting fraudulent anomalies. Numerous research endeavors employing diverse artificial intelligence techniques, such as deep learning and machine learning, have underscored the efficacy of this technology in enhancing the precision of fraud detection in the realm of banking transactions. Several scholarly studies have placed emphasis on the significance of model interpretability in the context of enhancing fraud detection capabilities, particularly in the realm of credit card fraud. Notably, Achituve [9] has explored the utility of the Hierarchical Attention Mechanism, Lucas [17] has investigated the potential of Hidden Markov Models (HMM), and Mao [26] has delved into the application of Graph Neural Networks (GNN) for this purpose. The detection of credit card activity has emerged as a prominent subject of discussion in various academic studies. This is mostly due to the ongoing vulnerability of credit card activities to potential fraudulent activities. Consequently, numerous researchers have explored the application of artificial intelligence (AI) in the detection of credit card fraud [15, 25, 28, 31].

Based on the findings of the study, it can be observed that the capital market occupies the second position in terms of sector ranking, positioned below the financial industry. The field of AI-based fraud detection in capital markets encompasses various methodologies that incorporate machine learning, deep learning, and data mining techniques. These methodologies employ an integration approach or model to evaluate the potential for financial fraud by employing risk-based assessment strategies [18, 22]. Additionally, a fraud-detection algorithm model is utilized to analyze financial statements for the purpose of identifying fraudulent activities [33, 37]. The effectiveness and capability of both models in detecting suspicious conduct that may lead to financial losses for entrepreneurs in the capital market were evaluated.

Moreover, this study has revealed that the utilization of AI-based fraud detection has extended to the E-Commerce, securities, and sports industries, albeit to a lesser extent. The e-commerce industry is considered one of the top industries, after the financial sector. Within this industry, there is ongoing research focused on detecting fraudulent activities using artificial intelligence (AI). Various approaches and methodologies, such as machine learning, have been explored to build prediction algorithms [2] and k-NN methods for this purpose [23]. Moreover, according to the findings of the aforementioned study, the securities and sports industries emerge as the least significant sectors. Both sectors have emerged as research subjects for the application of artificial intelligence in fraud detection. The utilization of artificial intelligence (AI) in fraud detection inside securities firms involves the implementation of a neural network system derived from the data mining domain. The outcomes of employing this technology have been reported as beneficial in the identification and prevention of fraudulent activities [36]. In contrast, the utilization of artificial intelligence (AI) for the identification of fraudulent anomalies yields advantageous outcomes for organizations operating in the sports sector. This is particularly evident in the integration of AI into enterprise resource planning (ERP) systems, which enables the detection of fraudulent indicators and warning signs through machine learning techniques. This implementation serves to safeguard companies from potential harm caused by fraudulent activities [29].

The utilization of machine learning has emerged as a prevalent methodology in numerous research endeavors. This study provides evidence of the growing popularity of machine learning in the integration of artificial intelligence-based technology for fraud detection in the financial sector. The results of this study reveal that 19 articles have been identified, which specifically examine the application of machine learning techniques in detecting fraudulent activities across diverse business domains. Numerous scholarly investigations have examined the utilization of machine learning, employing diverse methods, models, and approaches. Notably, prior researchers have predominantly employed predictive algorithm-making models, which have demonstrated efficacy in forecasting instances of fraud [18, 19, 21, 23, 25, 28, 31, 33, 34, 35, 37]. Furthermore, the integration of artificial intelligence in fraud detection within diverse financial sectors involves the utilization of Deep learning and Data mining techniques. The application of these methods has demonstrated their capability and effectiveness in identifying anomalies and indicators of fraudulent activities [2, 9, 15, 36, 37].

In general, extant literature demonstrates that artificial intelligence holds significant promise in enhancing the efficacy of financial fraud detection across many industries. The models presented in this work demonstrate a notable level of precision in detecting fraudulent transactions, while also enhancing comprehension of the patterns and behaviors linked to financial fraud. Furthermore, some studies have also examined the significance of taking into account the contextual factors and unique attributes of a specific industry to enhance the effectiveness of fraud detection methods [37]. Conversely, it has been argued that the utilization of artificial intelligence (AI) for fraud detection in the financial domain necessitates the involvement of financial professionals to conduct sophisticated analyses in identifying such fraudulent activities [36].

5. Conclusion

Artificial Intelligence can be conceptualized as a simulated manifestation of human cognitive abilities, which is emulated within a machine and governed by a programmed framework aimed at mimicking human thought processes. Artificial Intelligence (AI) refers to a computer-based system that possesses the ability to do tasks often associated with human resources or intelligence. The viability of AI intelligence is contingent upon the acquisition of experience and data necessary for optimal operational efficiency. In contrast to human operators who may not consistently provide explicit guidance to the AI learning process, artificial intelligence has the capacity to autonomously acquire knowledge through the assimilation of experiential data obtained during its utilization by humans, which is subsequently integrated via diverse automation frameworks. The utilization of artificial intelligence in the detection of financial fraud offers substantial advantages to the implementing entity, resulting in considerable outcomes. This paper presents a comprehensive review of 24 prior studies conducted between 2014 and 2023, focusing on the application of artificial intelligence (AI)-based fraud detection systems.

AI-driven systems for financial fraud detection have been implemented across diverse sectors, including the financial sector, capital markets, securities, and other industries, where the financial sector is the largest sector in adopting AI in detecting fraud. In addition, machine learning approach is one of the most widely used algorithmic methods and predictive technologies to identify and prevent fraud by several entities based on previous research. The effectiveness of implementing AI in identifying and detecting fraud lies in its ability to swiftly screening vast amounts of data, scaling patterns, and discern an odds that may predict some fraudulent activities. Through machine learning algorithms, AI systems can continuously learn from new data and adapt to evolving fraud techniques, enhancing their accuracy over time. Moreover, AI can automate routine tasks, enabling fraud analysts to focus on investigating more complex cases, thereby increasing operational efficiency.

Future investigations may prioritize the examination of the efficacy of artificial intelligence (AI) methodologies in the identification and mitigation of financial fraudulent activities. Additionally, it would be beneficial to analyze the societal, economic, and security ramifications associated with the integration of AI technologies into virtuous systems. Subsequent research endeavors may delve into the advancement of intricate and adaptable artificial intelligence models in order to effectively tackle progressively intricate patterns of fraudulent activities. In general, this study has the potential to offer a more extensive framework for the utilization of artificial intelligence in bolstering financial security and safeguarding assets against fraudulent risks.

References

[1] Sudarmanto E. Manajemen risiko: Deteksi dini upaya pencegahan fraud [Risk management: Early detection of fraud prevention efforts]. Jurnal Ilmu Manajemen. 2020;9(2):107-121. https://doi.org/10.32502/jimn.v9i2.2506. (Indonesian)

[2] Li J, Li N, Xia T, Guo J. Textual analysis and detection of financial fraud: Evidence from Chinese manufacturing firms. Economic Modelling. 2023;126:106428. https://doi.org/10.1016/j.econmod.2023.106428

[3] Sun H, Li J, Zhu X. Financial fraud detection based on the part-of-speech features of textual risk disclosures in financial reports. Procedia Computer Science. 2023;221:57-64. https://doi.org/10.1016/j.procs.2023.07.009

[4] Yan M, Filieri R, Gorton M. Continuance intention of online technologies: A systematic literature review. International Journal of Information Management. 2021;58:102315. https://doi.org/10.1016/j.ijinfomgt.2021.102315

[5] Pinto SO, Sobreiro VA. Literature review: Anomaly detection approaches on digital business financial systems. Digital Business. 2022;2(2):100038. https://doi.org/10.1016/j.digbus.2022.100038

[6] Zhang D, Frei R, Senyo PK, et al. Understanding fraudulent returns and mitigation strategies in multichannel retailing. Journal of Retailing and Consumer Services. 2023;70:103145. https://doi.org/10.1016/j.jretconser.2022.103145

[7] Abedini A, Salimi M, Mazaheri Y, et al. Assessment of cheese frauds, and relevant detection methods: A systematic review. Food Chemistry: X. 2023;19:100825. https://doi.org/10.1016/j.fochx.2023.100825

[8] Wyrobek J. Application of machine learning models and artificial intelligence to analyze annual financial statements to identify companies with unfair corporate culture. Procedia Computer Science. 2020;176:3037-3046. https://doi.org/10.1016/j.procs.2020.09.335

[9] Achituve I, Kraus S, Goldberger J. Interpretable online banking fraud detection based on hierarchical attention mechanism. IEEE 29th International Workshop on Machine Learning for Signal Processing (MLSP) [Internet]; 2019 Oct 13-16; Pittsburgh, PA, USA. New Jersey: IEEE; 2019 [cited 2023 Jun 3]. 6 p. Available from: https://doi.org/10.1109/MLSP.2019.8918896

[10] Akmaluddin M, Dewayanto T. Systematic literature review: Implementasi artificial intelligence dan machine learning pada bidang akuntansi manajemen [Systematic literature review: Implementation of artificial intelligence and machine learning in the field of management accounting]. Diponegoro Journal of Accounting. 2023;12(4):1-11. (Indonesian)

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

[12] Murima WH, Prayogi ARY, Rahvy AP, Djunaedi N, Dhamanti I. Telemedicine use in health facility during covid-19 pandemic: Literature review. Indonesian Journal of Health Administration. 2022;10(2):251-260. https://doi.org/10.20473/jaki.v10i2.2022.251-260

[13] Lame G. Systematic literature reviews: An introduction. Proceedings of the Design Society: International Conference on Engineering Design. 2019;1(1):1633-1642. https://doi.org/10.1017/dsi.2019.169

[14] Page MJ, McKenzie JE, Bossuyt PM, et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ. 2021;372:n71. https://doi.org/10.1136/bmj.n71

[15] Osegi EN, Jumbo EF. Comparative analysis of credit card fraud detection in simulated annealing trained artificial neural network and hierarchical temporal memory. Machine Learning with Applications. 2021;6:100080. https://doi.org/10.1016/j.mlwa.2021.100080

[16] Domashova J, Zabelina O. Detection of fraudulent transactions using SAS Viya machine learning algorithms. Procedia Computer Science. 2021;190:204-209. https://doi.org/10.1016/j.procs.2021.06.025

[17] Lucas Y, Portier P-E, Laporte L, et al. Towards automated feature engineering for credit card fraud detection using multi-perspective HMMs. Future Generation Computer Systems. 2020;102:393-402. https://doi.org/10.1016/j.future.2019.08.029

[18] Lu Q, Fu C, Nan K, et al. Chinese corporate fraud risk assessment with machine learning. Intelligent Systems with Applications. 2023;20:200294. https://doi.org/10.1016/j.iswa.2023.200294

[19] Canhoto AI. Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective. Journal of Business Research. 2021;131:441-452. https://doi.org/10.1016/j.jbusres.2020.10.012

[20] Zhu X, Qin XAZ, Chang Y, Liu Y, He Q, Li J. Intelligent financial fraud detection practices post- pandemic era. The Innovation. 2021;2(4):100176. https://doi.org/10.1016/j.xinn.2021.100176

[21] Moreira MÂL, Junior CSR, Silva DFL, et al. Exploratory analysis and implementation of machine learning techniques for predictive assessment of fraud in banking systems. Procedia Computer Science. 2022;214:117-124. https://doi.org/10.1016/j.procs.2022.11.156

[22] Lokanan ME, Sharma K. Fraud prediction using machine learning: The case of investment advisors in Canada. Machine Learning with Applications. 2022;8,:100269. https://doi.org/10.1016/j.mlwa.2022.100269

[23] Karunachandra B, Putera N, Wijaya SR, Suryani D, Wesley J, Purnama Y. On the benefits of machine learning classification in cashback fraud detection. Procedia Computer Science. 2023;216:364-369. https://doi.org/10.1016/j.procs.2022.12.147

[24] Chen L, Jia N, Zhao H, Kang Y, Deng J, Ma S. Refined analysis and a hierarchical multi-task learning approach for loan fraud detection. Journal of Management Science and Engineering. 2022;7(4):589-607. https://doi.org/10.1016/j.jmse.2022.06.001

[25] Chen K, Yadav A, Khan A, Zhu K. Credit fraud detection based on hybrid credit scoring model. Procedia Computer Science. 2020;167:2-8. https://doi.org/10.1016/j.procs.2020.03.176

[26] Mao X, Liu M, Wang Y. Using GNN to detect financial fraud based on the related party transactions network. Procedia Computer Science. 2022;214:351-358. https://doi.org/10.1016/j.procs.2022.11.185

[27] Misra S, Thakur S, Gosh M, Saha SK. An autoencoder based model for detecting fraudulent credit card transaction. Procedia Computer Science. 2020;167:254-262. https://doi.org/10.1016/j.procs.2020.03.219

[28] Izotova A, Valiullin A. Comparison of Poisson process and machine learning algorithms approach for credit card fraud detection. Procedia Computer Science. 2021;186:721-726. https://doi.org/10.1016/j.procs.2021.04.214

[29] Arslan E, Güneş A. Fraud detection in enterprise resource planning systems using one-class support vector machine combined with convolutional neural network: The case of Spor Istanbul. Annals of Applied Sport Sciences. 2023;11(S1). http://dx.doi.org/10.61186/aassjournal.1222

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

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

[32] Li J. E-commerce fraud detection model by computer artificial intelligence data mining. Computational Intelligence and Neuroscience. 2022;2022:8783783. https://doi.org/10.1155/2022/8783783

[33] Lokanan M, Tran V, Vuong NH. Detecting anomalies in financial statements using machine learning algorithm: The case of Vietnamese listed firms. Asian Journal of Accounting Research, 2019;4(2):181-201. https://doi.org/10.1108/AJAR-09-2018-0032

[34] Patil S, Nemade V, Soni PK. Predictive modelling for credit card fraud detection using data analytics. Procedia Computer Science. 2018;132:385-395. https://doi.org/10.1016/j.procs.2018.05.199

[35] Halvaiee NS, Akbari MK. A novel model for credit card fraud detection using artificial immune systems. Applied Soft Computing. 2014;24:40-49. https://doi.org/10.1016/j.asoc.2014.06.042

[36] Lin C-C, Chiu A-A, Huang SY, Yen DC. Detecting the financial statement fraud: The analysis of the differences between data mining techniques and experts' judgments. Knowledge-Based Systems. 2015;89:459-470. https://doi.org/10.1016/j.knosys.2015.08.011

[37] Chen Y-J, Wu C-H, Chen Y-M, Li H-Y, Chen H-K. Enhancement of fraud detection for narratives in annual reports. International Journal of Accounting Information Systems. 2017;26:32-45. https://doi.org/10.1016/j.accinf.2017.06.004