SYSTEMATIC LITERATURE REVIEW: DETECTION OF FINANCIAL FRAUD BASED ON MACHINE LEARNING

Anita*[1], Grace T. Pontoh[2], Gagaring Pagalung[3]
[123]Faculty of Economics and Business, Hasanuddin University, Indonesia
*Coresponden Email: Imanitaad13@gmail.com

ABSTRACT

Financial fraud detection is an important focus amid the increasing threat of digital fraud and the complexity of financial transactions. The study conducted *a Systematic Literature Review* (SLR) of 47 Scopus Q1 and Q2-indexed scientific articles published between 2015 and 2025, to identify *the machine learning methods*, the most frequently researched types of cheating, and the evaluation metrics used. The SLR process is applied according to the Kitchenham protocol and the PRISMA framework to maintain the validity and replication of the study. The results of the review show that *the Support Vector Machine* (SVM), *Artificial Neural Network* (ANN), and *Logistic Regression* (LR) algorithms are most commonly used, especially in the case of *credit card fraud, financial statement fraud,* and *insurance fraud*. Model evaluation generally uses *accuracy, precision, recall, F1-score*, and *AUC metrics*. This research makes an important contribution to mapping trends, dominant approaches, and research gaps regarding machine learning-based financial fraud detection, so that it can be useful as a strategic reference for the development of more adaptive and efficient detection systems in the future.
Keywords: *Machine Learning, Financial Fraud Detection, Systematic Literature Review, Financial Reports, Financial Transactions.*

INTRODUCTION

The act of obtaining financial benefits through unlawful and fraudulent means is known as financial fraud (Hilal et al., 2022). This type of fraud can occur in various sectors, including in the fields of insurance, banking, taxation, and in the corporate world (Aziz et al., 2022). In recent times, fraudulent practices in financial transactions (Lee, 2018), money laundering, and other forms of financial fraud, are increasingly becoming a serious problem among business actors and industry (Lee, 2018). Although various efforts have been made to suppress financial fraud activities, the reality is that this practice is still ongoing and has a negative impact on economic stability and people's lives, because every day there is a lot of money lost due to fraud (Tubb et al., 2018). Efforts to detect fraud have actually been developed for a long time (Hilal et al., 2022), but the traditional methods used tend to be manual, so they are inefficient because they take a long time, cost a lot of money, are less accurate, and are difficult to implement (Al-hashedi & Magalingam, 2021).

Research to reduce losses from fraudulent activities continues, but its effectiveness is still low. As artificial intelligence (AI) technology develops, the use of *Machine Learning* and *Data mining* Started to be applied in the fraud detection process in the financial sector (Chaquet-ulldemolins et al., 2022). various methods, both *Supervised* And *Unattended* has been used to identify fraudulent acts (Zeng, 2021). Among these various approaches, the classification method is the most commonly used technique in identifying suspicious financial transactions. This process begins with training the model using data that has been equipped with class labels and certain features. Once the model is trained, the test data will be classified in the next stage (Ashtiani & Rahemi, 2022).

Therefore, this study aims to identify Techniques based on *Machine Learning* which is used in detecting fraud in financial transactions, as well as analyzing research gaps to find

research trends in this field. In recent times, a number of studies have been conducted to detect financial fraud activities (Delamaire et al., 2019). Research conducted by (Delamaire et al., 2019) Conduct a study of the various types of credit card fraud, such as bankruptcy and counterfeiting, and recommend appropriate approaches to deal with them. (Phua et al., 2016) also researching the *Machine Learning* which is used to detect fraudulent transactions, including in the stock market and other fraud detection processes in the financial sector. In addition, it explores several approaches *Learn* which is specifically applied to detect fraud on credit cards. Also conducted comprehensive surveys to explore Engineering *Data mining* and *Machine Learning* in detecting various types of fraud such as credit card fraud, insurance fraud, and telecommunication service subscription fraud.

(West & Bhattacharya, 2016) It shows that there has recently been a significant spike in fraud cases in the health sector. In an effort to overcome this,(West & Bhattacharya, 2016) conduct research that focuses on a variety of statistics to identify fraudulent activity in the healthcare system. Meanwhile, (Wu et al., 2025) compile a comprehensive review of credit card fraud detection, reviewing various classification methods *Machine Learning*, including the methodology used and the challenges faced. (Tubb et al., 2018) reviewed a number of advanced methods used to detect fraud in payment card transactions through transaction volume analysis, and the results were only eight methods that were rated to be real-world in the industry. Next (Aziz et al., 2022) evaluate a number of studies over the past ten years that address fraud detection in the financial sector with an approach to *Data mining*. However, the review has not been considered thorough because it does not include the evaluation of the method as well as the advantages and disadvantages of the technique *Data mining* used.

Although a number of literature reviews have been conducted in this area, most research is still limited to specific areas of the financial world, such as credit fraud detection (Gyamfi, 2018), fraud in digital banking services, fraud in bank credit management, and fraud in payment cards (Patil et al., 2018). This shows the need for studies that cover the entire spectrum of financial fraud activities to bridge the existing research gap. Research (Ashtiani & Raahemi, 2022) review various methods of fraud detection in financial records and incorporate cross-disciplinary literature on financial statement fraud. However, there are a number of differences between their review and this study.

While many studies (West & Bhattacharya, 2016), (Phua et al., 2016) and (Ashtiani & Raahemi, 2022) have investigated ML based fraud detection, most have focused narrowly on specific domains such as credit card or insurance fraud. However, a comprehensive synthesis that integrates different ML techniques, performance metrics, and fraud typologies across financial sectors remains limited. Furthermore, exing reviews rarely discuss the methodological or research trends that guide algorithmic improvement.

The motivation of this study to bridge these fragmented findings and offer a systematic and comparative review of financial fraud detection using ML techiques. This study aims to (1) identify ML based approaches and algorithms commonly applied in fraud detection. (2) explore their performance evaluation metrics, and (3) highlight existing gaps to guide future research. By providing a broader and more analytical mapping of research patterns, dominant algorithms, and methodological developments, this study ectends prior works and support both theoretical understanding and practical implementation in detecting financial fraud more effectively.

METHODOLOGY

This study uses the *Systematic Literature Review* (SLR), which is a method that is systematically designed to collect and analyze various studies that answer certain research questions. The purpose of using this approach is to identify and integrate information relevant

to specific issues to reduce bias, present high-quality evidence-based reviews and facilitate the navigation of researchers' assessment and conclusion flows. The process of searching literature in this study was carried out systematically by following the identification stages within the framework of PRISMA (*Optional Reporting Items for Systematic Review and Meta Analysis*) as proposed by (Page et al., 2021). The article search is focused on scopus-indexed scientific articles, which are known to have a reputation as a credible source of academic literature. The design of this study follows the framework of the (Kitchenham & Charters, 2007), which divides the SLR process into three core stages: the review planning stage, the execution of the review and the reporting of the review results.

a. Stages of review planning

The planning stages in SLR include the preparation and development process, which consists of determining research objectives and systematically drafting review protocols (Ashtiani & Raahemi, 2022). To obtain articles relevant to the research topic, an automated search was conducted on a number of major digital databases that were considered most appropriate (Isong & Bekele, 2013). Other similar databases are not used because they are not considered the primary source of data indexes. The selection of the database was based on its high level of popularity and the completeness of the articles related to the research questions in this study. To ensure that the articles obtained are comprehensive and up-to-date, the time range used as a reference in this literature review is from 2014 to 2025.

b. Survey implementation

After the planning stage is completed, the next stage is the implementation of the review. At this stage, the main process in SLR begins to be carried out, namely by identifying research questions (*RQ)* that are the main focus in research discussion and analysis. In this phase, the procedure for selecting search strategies, as well as data extraction and synthesis procedures is also explained. A more detailed explanation of these aspects is presented in the next subsection.

1) Research Questions

The research questions in this SLR are set in advance to identify the main issues discussed and analyzed. The existence of research questions is very important in determining the main study to be reviewed. The preparation of research questions is generally a core component in the implementation of SLR. The main research questions used in this study are as follows:

Table 1 Research Questions

Not	Research Questions
1	What are the common types of financial fraud discussed based on *the Machine Learning* approach?
2	What is the *Machine Learning* approach that is often used to detect financial fraud?
3	What are the performance evaluation metrics used to detect financial fraud using *machine learning*?

The first question aims to find out the financial fraud that is most often discussed with *a machine learning approach.* The second question focuses on efforts to identify *machine learning* methods that are commonly used in detecting fraudulent financial activities. Meanwhile, the third and fourth questions were used to trace the performance evaluation metrics used in the detection of *machine learning fraud*.

2) Search strategy

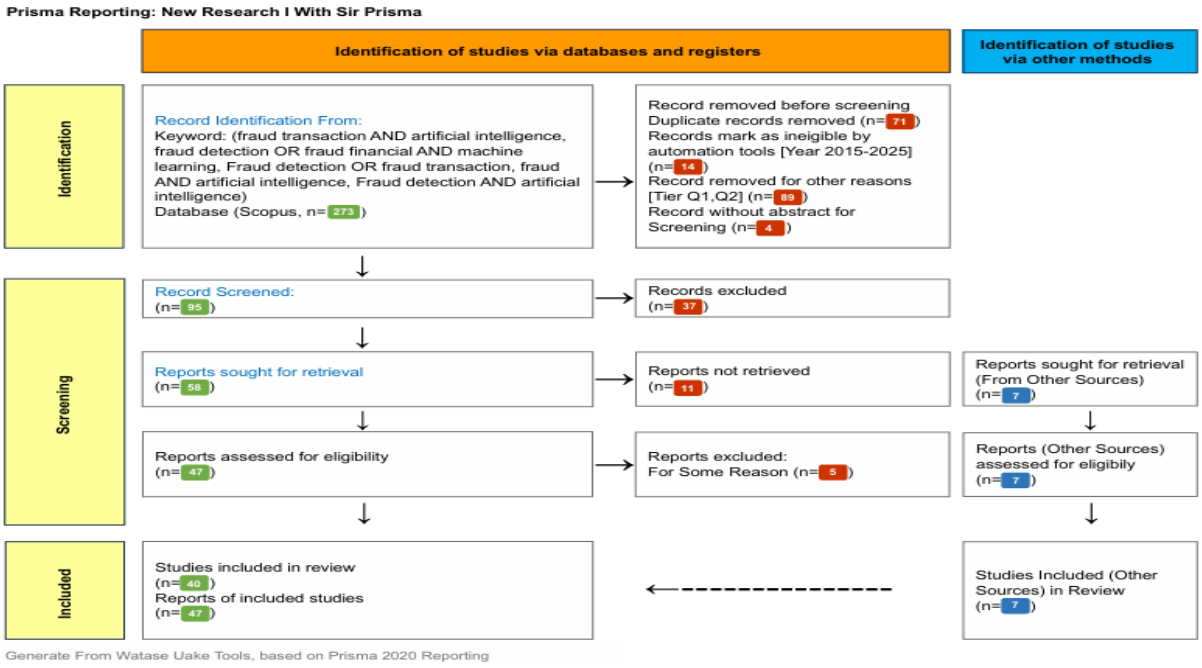
To find the most relevant articles related to machine learning (ML)-based financial fraud detection, the researcher designed a number of keywords that corresponded to the research question (RQ). Involves using Boolean terms such as "OR" and "AND" to combine keywords relevant to RQ. Some of the keywords used in this SLR include: "*Financial*

fraud"AND"*Financial transactions*"AND"*fraud detection"* AND "*Machine Learning*" OR "*Artificial intelligence*". The literature search process in this study was carried out systematically by following the identification stages in the PRISMA framework as proposed by (Page et al., 2021).

3) Application of criteria

After applying the search terms to the mentioned database, 273 were found. Of these, 71 articles were identified as duplicates and deleted, 14 were excluded from the vulnerable research period, 89 articles were not indexed Q1 and Q2, and 4 articles did not have abstracts, then the selection process continued by screening the remaining 95 articles, in this selection stage, the authors applied inclusion criteria to ensure that the selected articles were really relevant. The screening process is carried out based on the remaining 95 articles, which are then assessed according to the quality standards that have been determined. This quality assessment aims to ensure that the selected articles do meet the criteria that can guarantee the credibility of the research results, all stages of quality assessment selection are carried out, as many as 47 articles are ensured to be feasible and relevant to the research question.

Figure 1 PRISMA Selection Process



The criteria for the selected articles can be seen in Table 2 below:

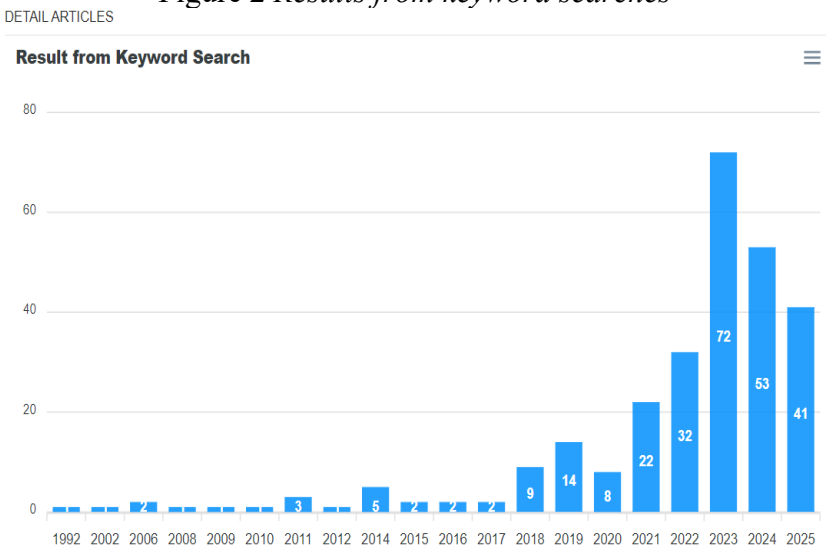
Not	Article Criteria
1	Published articles and Scopus Q1 & Q2 indexed journals for the period 2015 to 2025
2	Articles that discuss financial fraud detection and applying *Machine Learning methods*
3	Articles available in English in full
4	Accessible articles

4) Study decryption

The number of articles found based on keyword search results from 2015 to 2025 is presented in figure 2. This graph illustrates the trend of publications related to the topics studied in this study. Before 2017, the number of publications was still very low and fluctuating, but

since 2018 the trend has begun to increase sharply, with the highest spike occurring in 2023 as many as 72 articles. Despite the decline in 2024 and 2025, the number of articles remains high, namely 53 and 41 articles. These findings show that the research topics studied are increasingly attracting the attention of academics, especially since the last five years.

Figure 2 *Results from keyword searches*



RESULT AND DISCUSSION

This section presents the stages of selecting articles that are considered relevant in this SLR research.

RQ1 What are some common types of financial fraud that are discussed based on *the Machine Learning* approach?

The type of fraudulent activity found is highly dependent on a particular industry sector (Ashtiani & Raahemi, 2022)(Nassif et al., 2021). To answer the RQ1 question, this section presents the different forms of fraudulent activity identified and addressed using the *Machine Learning*, as listed in the article that has been reviewed. From the results of the review, fraudulent activities in the financial sector can be broadly divided into several categories, namely credit card fraud, mortgage fraud, financial statement fraud, and fraud in health services. The following table 3 shows a summary of the different types of financial fraud to be mentioned.

Table 3 Types *of Financial Fraud*

Types of Scams	Description	Techniques Used	Reference
Financial statement fraud	It is a corporate fraud in which financial statements are illegally modified to make the organization look more profitable.	*Supports Vector Engine, Fuzzy Logic, decision tree, genetic algorithms, regression logistics, markov mode.*	(Ashtiani & Raahemi, 2022), (Li et al., 2024), (Lin, 2024), (Schneider & Brühl, 2023), (West & Bhattacharya, 2016), (Latipov et al., 2025), (Zhao & Bai, 2022), (Zhu et al., 2025), (Hamal & Senvar, 2021)

Credit card fraud	Use of the card without permission from the rightful owner	*Supports Vector engines, fuzzy logic, clustering-based methods, Hedden Markov models, decision trees, artificial neural networks, genetic algorithms, random forests, logistic regression.*	(Al-hashedi & Magalingam, 2021), (Alamri & Ykhlef, 2024),(Almazroi & Ayub, 2023),(Charizanos et al., 2024), (Faraji, 2022), (Hilal et al., 2022), (Mim et al., 2024), (Nassif et al., 2021), (Phua et al., 2016), (Salam, 2024), (Talukder et al., 2024), (Tubb et al., 2018), (Randhawa et al., 2018), (West & Bhattacharya, 2016), (Alwadain & Ali, 2023), (Chaquet-ulldemolins et al., 2022), (Latipov et al., 2025), (Mienye & Swart, 2024), (Kanika et al., 2022)
Health insurance scams	False claims by individuals or organizations to support unauthorized spending or intentional damage	*Supports Vector engines, cluster-based methods, K Neghbors Nearby, naïve bayes, decision trees, artificial neural networks,*	(Al-hashedi & Magalingam, 2021), (Hilal et al., 2022), (Phua et al., 2016), (Talukder et al., 2024), (Tubb et al., 2018), (West & Bhattacharya, 2016)
Cyber financial fraud	Financial fraud activities through cyberspace	*Support Vector engine*	(Firdaus et al., 2022), (Nassif et al., 2021), (Btoush et al., 2025)
Other scams	Other frauds in the financial field include commodity and securities fraud, mortgage fraud, corporate fraud, and money laundering	*Support Vector engine, decision tree, fuzzy logic, hidden markov model*	(Chithanuru & Ramaiah, 2025), (Hilal et al., 2022), (Usman et al., 2024), (Aghili et al., 2022), (Ahmed & Alrasheed, 2025), (Binsawad, 2025), (Dichev & Zarkova, 2025), (Mohammed et al., 2023),

Credit card fraud

Electronic financial transactions that do not use cash directly often involve credit users. *Credit card fraud* is a scam that involves illegal transactions using credit cards, both online and offline (Al-hashedi & Magalingam, 2021). Criminals use these cards to make illegal transactions, which can result in huge losses for both banks and cardholders. In fact, the existence of fake credit cards makes it easier for fraudsters to carry out their activities illegally (Salam, 2024), (Talukder et al., 2024). In general, using a credit card without the permission of its rightful owner is considered an illegal act (Alwadain & Ali, 2023). When a person gains access to a certain account in an illegal way and makes a transaction, then the action to a certain account in an illegal way and makes a transaction, then the action is categorized as fraud (Faraji, 2022), (Hilal et al., 2022). The types of fraud using credit cards can be divided into two categories, namely offline and online fraud. In offline fraud, stolen credit cards are used by perpetrators to make transactions as if they were the original owners. Meanwhile, in online fraud, perpetrators

use the internet to carry out their actions (Hilal et al., 2022), (Mim et al., 2024), (Nassif et al., 2021), (Phua et al., 2016).

Financial Statement *Fraud*

Fraud in financial statements includes the act of falsifying financial statements to give the impression that a company has better performance than it actually (Schneider & Brühl, 2023). The goals include avoiding paying taxes, increasing stock prices, or obtaining loans from banks (Hamal & Senvar, 2021). These financial statements can be thought of as confidential records compiled by the organization and contain information regarding expenses, profits, income, and loans (Li et al., 2024). In addition, the report also includes a summary compiled by management regarding business performance as well as predictions of future business direction. Various financial reports usually manipulate this information to make it look profitable for report users. The main purpose of this falsification of financial statements is to increase the price of the stock, reduce the tax burden, attract as many investors as possible, as well as obtain personal loans from banks and other interests (Latipov et al., 2025), (Zhao & Bai, 2022), (Zhu et al., 2025)(Lin, 2024).

Insurance Fraud

Insurance fraud is a false claim of loss in order to get money from an insurance company. This includes false claims for car accidents, health, agriculture and others (Al-hashedi & Magalingam, 2021) (Hilal et al., 2022). Generally, insurance serves to protect individual or organizational transactions against unexpected financial risks. The main targets of insurance fraud claims include health insurance. And motor vehicle insurance. Although fraud also occurs in home and property insurance, literature on this topic is still limited (West & Bhattacharya, 2016). It is estimated that the total losses due to insurance fraud in the United States reach more than one billion USD per year which ultimately leads to an increase in insurance premiums for consumers (Hilal et al., 2022). To legally identify claims for loss or damage to a vehicle, it usually takes an opportunity between the insurance company and the policyholder, both individuals and organizations. Fraudsters can act alone and commit fraud through misleading means during the claim process. In addition, there are also organized groups that work together to run insurance fraud. Generally, this group carries out fake incidents or fabricated accidents, in some cases, the accident does not even actually happen, but rather the vehicle that is brought to the scene of the incident (Phua et al., 2016), (Talukder et al., 2024), (Tubb et al., 2018).

Most cases of fraud are opportunistic, where the perpetrator takes advantage of the situation without prior planning, for example by exaggerating the claim of damage or loss experienced. Another type of insurance fraud that often occurs is in the healthcare sector (Al-hashedi & Magalingam, 2021). This sector is an important issue in modern society because it concerns social, political, and economic issues. The high cost of meeting the demand for quality medical services and the technology needed is also a burden in itself. In addition, many low-income families rely heavily on health insurance programs provided by the government to cope with rising medical costs, including the cost of prescription drugs and health services (Talukder et al., 2024),.

Financial Cyber Fraud (*Financial Cyber Fraud*)

Term *Financial Cyber Fraud* refers to crimes committed through cyberspace with the aim of obtaining economic benefits illegally (Btoush et al., 2025). The perpetrators of these financial

cybercrimes are difficult to detect. Usually, they disguise their actions to resemble the normal behavior of other financial service users, but when these actions are combined, there are irregularities. As technical and technological skills develop, it is increasingly difficult to detect and fight these crimes, as perpetrators continue to innovate to evade security systems (Nassif et al., 2021). Therefore, financial companies now prefer to use in-house technology to protect their assets, such as the use of tools to analyze data and detect potential financial attacks. However, some models are still not able to handle the attack effectively, new methods are constantly being developed (Firdaus et al., 2022). This effort encourages organizations to better protect customer data, company assets, and their own reputations. These innovations in this field rely heavily on machine learning and deep learning models (*Deep Learning*) from industry and academia.

Other types of financial fraud

In addition to the types of fraud discussed earlier, there are several other forms of fraudulent activity in the financial sector. Among them are commodity and securities fraud, recruitment fraud, corporate fraud, and money laundering (Chithanuru & Ramaiah, 2025). Commodity and securities fraud occurs when someone in a company spreads false information for personal gain (Hilal et al., 2022). Fraud in the mortgage process occurs if there is a deliberate misinformation, either in the initial process or during the credit application process used by the risk loan officer. This scam deliberately targets consumers to trick them into providing false information in the loan application process.

Corporate fraud usually involves manipulation of financial documents by companies to give an image as if the company's finances are in good condition. Meanwhile, *Money Laundering* or money laundering is an act of disguising the origin of illegal funds by making it appear as if they come from legitimate activities (Chithanuru & Ramaiah, 2025). This practice is dangerous because it is often used to hide the proceeds of other crimes, such as drug trafficking and trafficking crimes. Other types are *Ponzi schemes*, which is an investment fraud scheme that provides profits to existing investors using funds from new investors. The main goal of this scheme is to attract more victims and divert illegal profits from existing investors to fraudsters (Binsawad, 2025), (Dichev & Zarkova, 2025), (Mohammed et al., 2023).

RQ2 What are some *of the Machine Learning* approaches that are often used to detect financial fraud?

Machine learning (ML) refers to an analytical technique that is able to find certain patterns without direct direction from an expert (Faraji, 2022). The detection of financial fraud has been extensively researched using the ML method by many researchers (Rb & Kr, 2021). Such as SVM, ANN, HMM, KNN, *Decision Tree*, and others. Therefore, to answer the second research question (RQ2), this section presents a sharing of popular ML methods used to detect financial fraud based on the articles studied. Detailed explanation of the Techniques *Mechine Learning* used to detect financial fraud activities are presented in the following subsection.

Table 4 Machine *Learning* techniques used to detect financial fraud

Technique	Description	Reference
SVM	Classification methods used in linear classification	(Al-hashedi & Magalingam, 2021), (Alamri & Ykhlef, 2024),(Almazroi & Ayub, 2023), (Ashtiani & Raahemi, 2022), (Chen & Wu, 2023), (Hilal et al., 2022), (Li et al., 2024), (Lin, 2024), (Mim et al., 2024), (Nassif et al., 2021), (Phua et al., 2016), (Schneider & Brühl, 2023), (Tubb et al., 2018), (Randhawa et al., 2018), (West & Bhattacharya, 2016), (Aghili et al., 2022), (Algani et al., 2022), (Alwadain & Ali, 2023), (Btoush et al., 2025), (Mohammed et al., 2023), (Zhao & Bai, 2022), (Zhu et al., 2025), (Zhou et al., 2019)
ANN	The multi-layered networks that work are similar to the way humans think.	Almazroi & Ayub, 2023), (Ashtiani & Raahemi, 2022), (Tubb et al., 2018), (Aghili et al., 2022)
Fuzzy logic	The logic that states that human thinking is approximate is not always accurate.	Almazroi & Ayub, 2023), (Charizanos et al., 2024)
KNN	Classify data based on its similarity or proximity.	(Alamri & Ykhlef, 2024), Almazroi & Ayub, 2023), (Ashtiani & Raahemi, 2022), (Chithanuru & Ramaiah, 2025), (Faraji, 2022), (Hilal et al., 2022), (Mim et al., 2024), (Salam, 2024), (Tubb et al., 2018), (Usman et al., 2024), (Algani et al., 2022), (Alwadain & Ali, 2023), (Binsawad, 2025), (Mohammed et al., 2023)
Decision Tree	Classification and regression methods are in the form of trees that are used to aid decision-making.	(Alamri & Ykhlef, 2024), (Faraji, 2022), (Hilal et al., 2022), (Li et al., 2024), (Mim et al., 2024), (Nassif et al., 2021), (Phua et al., 2016), (Tubb et al., 2018), (Randhawa et al., 2018), (West & Bhattacharya, 2016), (Alwadain & Ali, 2023), (Binsawad, 2025), (Btoush et al., 2025), (Mohammed et al., 2023), (Zhao & Bai, 2022), (Zhou et al., 2019)
Genetic Algorithms	Find the best solution to the problem by trying out a variety of possible solutions.	(Nassif et al., 2021), (West & Bhattacharya, 2016)
Ensemble	The combination of several artificial intelligence techniques into one prediction technique.	(Alamri & Ykhlef, 2024), (Ashtiani & Rahemi, 2022), (Chithanuru & Ramaiah, 2025), (Faraji, 2022), (Lin, 2024), (Phua et al., 2016), (Tubb et al., 2018), (Mytnyk et al., 2023), (Aziz et al., 2022)
Logistic Regression	A technique commonly used in binary or multi-class classification.	(Alamri & Ykhlef, 2024), Almazroi & Ayub, 2023), (Ashtiani & Rahemi, 2022), (Charizanos et al., 2024),(Chen & Wu, 2023), (Faraji, 2022), (Hilal et al., 2022), (Li et al., 2024), (Lin, 2024), (Mim et al., 2024), (Nassif et al., 2021), (Salam, 2024), (Schneider & Brühl, 2023), (Tubb et al., 2018), (Qiu & He, 2018), (Randhawa et al., 2018), (Usman

		et al., 2024), (West & Bhattacharya, 2016), (Alwadain & Ali, 2023), (Btoush et al., 2025), (Chaquet-ulldemolins et al., 2022), (Dichev & Zarkova, 2025), (Mohammed et al., 2023), (Song et al., 2020), (Zhao & Bai, 2022), (Mekterovi et al., 2021)
Clustering	Unsupervised learning methods that group similar data into a single group	(Phua et al., 2016)
Random Forest	Classification methods that combine multiple decision trees	(Alamri & Ykhlef, 2024), (Ashtiani & Rahemi, 2022), (Chen & Wu, 2023),(Chithanuru & Ramaiah, 2025), (Faraji, 2022), (Hilal et al., 2022), (Li et al., 2024), (Lin, 2024), (Mim et al., 2024), (Nassif et al., 2021), (Salam, 2024), (Schneider & Brühl, 2023), (Tubb et al., 2018), (Randhawa et al., 2018), (Alwadain & Ali, 2023), (Btoush et al., 2025), (Mohammed et al., 2023), (Zhao & Bai, 2022), (Zhu et al., 2025), (Hamal & Senvar, 2021)
The naïve Bayes	A classification algorithm that can predict the membership of a group	(Alamri & Ykhlef, 2024), Almazroi & Ayub, 2023), (Ashtiani & Rahemi, 2022), (Chithanuru & Ramaiah, 2025), (Hilal et al., 2022), (Mim et al., 2024), (Nassif et al., 2021), (Phua et al., 2016), (Salam, 2024), (Tubb et al., 2018), (Randhawa et al., 2018), (Usman et al., 2024), (West & Bhattacharya, 2016), (Alwadain & Ali, 2023), (Binsawad, 2025), (Mohammed et al., 2023), (Song et al., 2020), (Zhang et al., 2020)

Logistic Regression (*Logistic Regression*)

Technique *Logistic regression (LR)* Often used to solve binary and multi-class classification problems (Alamri & Ykhlef, 2024). LR works by regressing a set of variables to explain the patterns and relationships between binary dependent variables (Mohammed et al., 2023), (Song et al., 2020). LR is very useful for describing patterns and explaining the relationships between variables. In an article review by (Ashtiani & Raahemi, 2022), Logistic regression is one of the machine learning techniques (*Machine Learning*) most commonly used to detect errors in financial reporting (*Financial misrepresentation*). Based on the study, most studies chose to use LR in detecting financial fraud. A proper LR technique can help explain the characteristics or characteristics of fraudulent behavior in financial transactions, the proposed LR model performs well when compared to other detection methods (Li et al., 2024), (Lin, 2024), (Mim et al., 2024), (Nassif et al., 2021), (Salam, 2024), (Schneider & Brühl, 2023), (Tubb et al., 2018), (Qiu & He, 2018).

***Supports Vector Engine* (SMV)**

SMV is a supervised ML method (*supervised learning*) who are looking for *hyperplane* with a maximum margin to classify training data into two categories (Al-hashedi & Magalingam, 2021). This algorithm can classify new data based on predefined labels for each class (Chen & Wu, 2023), (Hilal et al., 2022). From the various studies reviewed, SMV has been applied by many researchers as an approach in detecting cheating. Example (Algani et al., 2022), developed a hybrid method that combines SMV algorithms with theory *Fusion Hazard* for

fraud detection purposes. Experimental results from (Zhao & Bai, 2022), (Zhu et al., 2025) shows that this approach is superior to other methods in terms of time efficiency and value *Size-F*. also applies the SMV Technique to detect fraud through an automated medical billing system. This method is designed to provide rapid detection of medical fraud *Real-time*. From the test results (Almazroi & Ayub, 2023), this model is proven to have better performance disband approaches before. Meanwhile, it utilizes SMV that has been optimized to detect fraudulent actions in online credit card transactions.

In this approach, some analyze the model's performance by using commercial bank business data. Research results (Aghili et al., 2022) shows that the SVM method provides better performance compared to other benchmark models, especially in terms of feasibility. proposes a method for detecting fraudulent transactions on credit cards by combining SVM and decision tree-based techniques. This approach aims to overcome the limitations of existing methods. Then, develop an SVM-based superior learning system that is able to distinguish legal and illegal customer behavior in credit card transactions. To improve detection accuracy, some researchers combine SVM methods, logic and linear regression (Schneider & Brühl, 2023) (Randhawa et al., 2018). using the VM method with an undersampling technique on the data, which is applied to detect fraud in the insurance industry. Meanwhile, developing a fraud detection model on credit cards by combining OSVM with deep learning methods (*Deep Learning*). The model is tested using real-world data and shows relevant results.

Bayesian Method

The Bayesian method (BN) is a type of graphical model that considers independent and conditional relationships between variables (West & Bhattacharya, 2016), (Alwadain & Ali, 2023). In this model, the network structure consists of nodes (*Node*) and lines (*Edge*) directed. Bayesian models are often used in anonymous probability calculations. Based on the literature reviewed, there are two main types of Bayesian methods, namely *Bayesian Belief Networks* and *Naif Bayes (NB)* (Alamri & Ykhlef, 2024), (Almazroi & Ayub, 2023). NB is *Machine Learning* (ML) is based on Bayes' theorem and is used to predict the probability of a data falling into a certain category. This model predicts the label of a data based on the probability that it falls into a certain category.

Some researchers have applied the NB model to detect financial fraud. For example, using the NB model to create a fraud detection model on financial transactions. Experiments were carried out with financial data that included normal and abnormal financial statements. The results show that this model is effective in detecting fraud. use NB algorithms to detect fraud in the healthcare sector, particularly in medical procedure records (Mim et al., 2024), (Nassif et al., 2021). The purpose of the research is to classify the behavior of health care providers, whether they are classified as normal or suspicious. To improve fraud detection performance, develop methods to detect fraudulent transactions by identifying important features of financial statements. In the experiment, the authors considered linguistic aspects as well as financial discussions in management reports. The results show that this model is better than other machine learning methods.

Decision Tree

Decision Tree (DT) is a machine learning (ML) technique used for decision-making based on tree structure, where each node represents a decision on a feature (Mohammed et al., 2023). Over the years, various methods have been developed using DT to detect financial fraud. (West & Bhattacharya, 2016) develop DT-based models to analyze credit card transactions, both normal and suspicious. The method was evaluated and compared with other approaches using

machine learning models. The results show that DT provides high performance in detecting suspicious transactions.

A study by (Tubb et al., 2018) compare three models: DT, *Random Forest* (RF), and *Induction Rules (RI)*, to detect insurance fraud. The results show that the DT model has the best accuracy in classifying fraudulent transactions. The transaction behavior of credit card holders to distinguish between normal and fraudulent transactions. The study compared different models, including DT, RI, and NB. The results of the evaluation show that *Random Forest (RF)* works better than DT. Another study also applied a DT-based approach to insurance fraud data, and the results were able to remove minority data classes in the insurance datasets used (Mohammed et al., 2023), (Zhao & Bai, 2022), (Zhou et al., 2019).

K-Nearest Neighbor (KNN) Algorithm

Algorithm *K-Nearest Neighbors* (KNN) is a machine learning technique (*Machine Learning*) supervised (*Supervised*) and is relatively simple, yet effective for both regression and classification processes (Usman et al., 2024), (Algani et al., 2022). In this method, class labels are determined based on a set of data that is closest (the closest neighbor) to the data being analyzed. KNN is a type of non-parametric model used for classification and regression tasks, by looking for the data that is closest to the position in a dataset and then making predictions based on the distance between those data (Almazroi & Ayub, 2023).

Although KNN works quite well on many types of datasets, its performance often degrades when the data used is unbalanced (*Balanced*). One of the popular methods used in calculating the distance between data is *Euclidean Distance* (Faraji, 2022). A number of up-to-date approaches have also been developed to improve the detection of financial fraud. develop a credit card fraud detection model using two approaches: the KNN model and the outlier detection model. The results of the experiment showed that the KNN model was more effective at detecting fraud in credit card transactions (Chithanuru & Ramaiah, 2025).

Research by (Ashtiani & Rahemi, 2022) It also uses the KNN algorithm to analyze credit card transactions and detect fraudulent behavior. They used credit card datasets from European users. The results of the study show that the model *K-Nearest Neighbors* provides better performance than other methods in this context. develop a KNN-based approach to detect fraud in the insurance sector. This approach combines three methods, namely *That is*, *Chebyshev-based*, *Density-based*and *Interquartile range* in detecting anomalies. This study also pays attention to the influence of feature selection (*Feature selection*) to the level of accuracy of the model.

Ensemble Method

Method *Ensemble* is a *meta-algorithm* that combines various artificial intelligence techniques in one predictive approach (Chithanuru & Ramaiah, 2025). The main goal of this method is to address the weaknesses of each individual model by combining them into a more powerful combined model. Each type of ensemble has a different function. Example *Increase* reduce prediction bias, *Bagging* lower variance, and *Arrange* Improve accuracy by combining several basic models (Alamri & Ykhlef, 2024).

Based on many reviewed articles, *Random Forest (RF)* Become a Technique *Ensemble* most commonly used for classification. RF has high performance because it combines the results of many decision trees and adjusts the final classification results based on majority voting. In the study (Phua et al., 2016), (Tubb et al., 2018), (Mytnyk et al., 2023), RF shows superior performance compared to other methods. One of the methods *Bagging* Other popular are *Bootstrap Aggregation (BA)*, which creates multiple samples from the training dataset

through the data retrieval technique. According to some studies, BA works better than a single learning approach. In categories *Increase*, *AdaboostMI* is one of the outstanding implementation examples. This method is used by to detect financial fraud. This technique repeats training on the dataset to generate *Classifier* stronger combination. Although it initially only used a simple model, the end result was able to match more complex ML methods.

Artificial Neural Network (ANN)

ANN is an information processing technique inspired by the way biological neural networks work (Tubb et al., 2018). ANN is very effective, especially when large amounts of data are available. A number of ANN-based models have been widely used to detect fraud in the financial sector. One example is research by (Aghili et al., 2022), that uses the ANN method to detect credit card fraud on the merchant side (*Trader*). The proposed model connects merchants with payment systems (*Payment gateway*). This payment system acts as an intermediary between merchants and customers, accessing customer credit card information and a built-in fraud detection model.

To detect other credit card frauds, develop a hybrid model based on *Cost-sensitive neural networks*. Results of the research (Ashtiani & Rahemi, 2022) shows that the model is able to increase fraud detection rates and reduce the number of false positive detection errors (*False positives*). (Almazroi & Ayub, 2023) also proposes a machine learning (ML)-based approach to detect fraud in credit card transactions. The study used a variety of ML algorithms, including the ANN model, which were applied to detect suspicious credit card transactions. The goal is to improve the security and accuracy of credit card auto-detection systems. introduce fraud detection methods by using *Multilayer Forward Feed Neural Network (MLFF)*. In addition, the ANN-based technique *Deep Reinforcement Learning (DRL)* It is also used in detecting fraud in the banking sector.

Fuzzy-Logic-Based Method

Fuzzy logic (FL) is an effective conceptual framework for dealing with problems full of uncertainty and ambiguity (Almazroi & Ayub, 2023). FL is a logic that recognizes that human ways of thinking are not always precise or definite. The combination of FL with other concepts has been proven to be able to provide a better and new approach to solving complex problems. Several fuzzy logic-based methods have been used in fraud detection according to (Charizanos et al., 2024) One of them is the model *FUZZ-GY hybrid* that combines fuzzy logic and behavioral models (*Behavioral models*) to detect unusual patterns in credit card transactions. This model assesses the characteristics of transactions and buyer habits. Behavioral logic is used to analyze buyer behavior in a variety of situations. In addition, another fuzzy approach focuses on the ability to understand the user's intentions and motivations.

Develop methods to detect fraud in credit card transactions by distinguishing between fraudulent and non-fraudulent transactions using fuzzy rules drawn from real data. This method successfully delineates the number of false positive detection errors. The performance of this model was also evaluated with an artificial neural network-based classification (ANN) approach. As a result, the combination of clustering and machine learning was able to improve accuracy and reduce false predictions. Based on experience to improve detection accuracy. This approach is able to recognize suspicious transaction patterns using fuzzy rules. Furthermore, it introduces *a fuzzy* logic-based approach that is integrated with feature *selection techniques* to improve detection performance.

Genetic Algorithm (GA)

Genetic algorithms (GAs) are inspired by the concept of natural evolution. This method works on the basis of a set of solutions that are usually represented in the form of binary strings such as chromosomes, and then through a selection process to find the best solution (West & Bhattacharya, 2016). Genetic programming falls into the category of evolutionary algorithms that expand the application of genetic methods to explore the various possibilities of computer programming optimally. GA has been widely used in the literature to detect financial fraud. For example, in (Nassif et al., 2021) implement GA to detect credit card fraud. Meanwhile, developing a new method that combines GA with *K-mean grouping* to detect fraudulent transactions, especially on unbalanced data (minority classes are fewer in number). *K-means* is used to group and classify minority data, then GA is applied to create new data within the group so that a more balanced training dataset is formed. In addition, it also implements GA to solve the problem of credit card fraud detection, using real transaction data from the real world.

Clustering-Based Methods (*Clustering-Based Methods*)

Clustering is a method of unsupervised learning (*Unsupervised learning*) that is used to group data that has similarities into the same group (Phua et al., 2016). Although the clustering technique is quite popular in detecting financial fraud, its implementation is still relatively small compared to the classification techniques discussed in the reviewed articles. Develop a model for detecting financial transaction fraud using the *Text mining* based on hierarchical clustering. They also propose a fraud detection approach by combining text dimension reduction and document clustering. Technique *Decomposition of Single Values* (SVD) is used to reduce the dimensions of the text. Furthermore, they developed a dual GHSOM technique to detect spatial patterns of decentralized fraud (*non-deceptive-central spatial hypothesis*) (Phua et al., 2016). This model is able to identify the topological patterns of fraudulent financial transactions. then combine the clustering method *K-means* and SOM (*Self-Setting Map*) to create cluster-based fraud detection methods. To overcome the weaknesses of SOMs that often face uncertainty within cluster boundaries, they also implemented K-means as an additional solution.

RQ3 What are the performance evaluation metrics used to detect financial fraud using *machine learning*?

To assess the performance of a model, evaluation metrics play an important role in detecting financial fraud (Alwadain & Ali, 2023). Nonetheless, there is no specific evaluation metric that is exclusively used to evaluate techniques *Machine Learning* in the context of fraud detection (Saleh et al., 2021). In recent times, many researchers use a variety of different performance evaluation metrics, such as accuracy, precision, *remember*, F *Score*, *False negative rate* (FNR), *area below the curve* (AUC), and specificity. In this section, various evaluation metrics used in the reviewed articles are presented. Table 5 shows the formula of each of these evaluation metrics.

Table 5 Evaluation metrics

Metric	Rumors	Reference
Accuracy	$Accuracy = \frac{(TN + TP)}{(TN + FN + FP + TP)}$	Almazroi & Ayub, 2023), (Ashtiani & Rahemi, 2022), (Chithanuru & Ramaiah, 2025), (Faraji, 2022), (Hilal et al., 2022), (Li et al., 2024), (Lin, 2024), (Mim et al., 2024), (Nassif et al., 2021), (Phua et al., 2016), (Salam, 2024), (Schneider & Brühl, 2023), (Talukder et al., 2024), (Randhawa et al.,

		2018), (Usman et al., 2024), (West & Bhattacharya, 2016), (Aghili et al., 2022), (Alwadain & Ali, 2023), (Binsawad, 2025), (Btoush et al., 2025), (Chaquet-ulldemolins et al., 2022), (Latipov et al., 2025), (Mohammed et al., 2023), (Song et al., 2020), (Wu et al., 2025), (Zhao & Bai, 2022), (Zhu et al., 2025), (Zhou et al., 2019), (Hamal & Senvar, 2021)
Precision	$Precison = \frac{TP}{(TP + FP)}$	(Al-hashedi & Magalingam, 2021), (Alamri & Ykhlef, 2024), (Chen & Wu, 2023), (Chithanuru & Ramaiah, 2025), (Faraji, 2022), (Hilal et al., 2022), (Lin, 2024), (Mim et al., 2024), (Nassif et al., 2021), (Phua et al., 2016) (Salam, 2024), (Talukder et al., 2024), (West & Bhattacharya, 2016), (Aghili et al., 2022), (Algani et al., 2022), (Binsawad, 2025), (Btoush et al., 2025), (Ekle & Eberle, 2025), (Latipov et al., 2025), (Mienye & Swart, 2024), (Mohammed et al., 2023), (Song et al., 2020), (Wu et al., 2025), (Zhao & Bai, 2022), (Zhu et al., 2025), (Zhou et al., 2019), (Zhang et al., 2020), (Mekterovi et al., 2021), (Hamal & Senvar, 2021)
Withdrawal / Sensitivity / TPR	$Recall = \frac{TP}{(TP + FN)}$	(Al-hashedi & Magalingam, 2021), (Alamri & Ykhlef, 2024), (Chithanuru & Ramaiah, 2025), (Faraji, 2022), (Hilal et al., 2022), (Lin, 2024), (Mim et al., 2024), (Nassif et al., 2021), (Phua et al., 2016) (Salam, 2024), (Schneider & Brühl, 2023), (Talukder et al., 2024), (Randhawa et al., 2018), (West & Bhattacharya, 2016), (Aghili et al., 2022), (Algani et al., 2022), (Binsawad, 2025), (Btoush et al., 2025), (Latipov et al., 2025), (Mienye & Swart, 2024), (Mohammed et al., 2023), (Wu et al., 2025), (Zeng, 2021), (Zhao & Bai, 2022), (Zhu et al., 2025), (Zhou et al., 2019), (Zhang et al., 2020), (Mekterovi et al., 2021), (Hamal & Senvar, 2021), (Kanika et al., 2022)(Aziz et al., 2022)
F-measure F1-Score	$F1 = 2\,x\,\frac{Recall\ x\ Precision}{(Recall + Precision)}$	(Al-hashedi & Magalingam, 2021), (Alamri & Ykhlef, 2024), (Charizanos et al., 2024), (Chithanuru & Ramaiah, 2025), (Faraji, 2022), (Hilal et al., 2022), (Mim et al., 2024), (Nassif et al., 2021), (Phua et al., 2016), (Salam, 2024), (Talukder et al., 2024), (Usman et al., 2024), (West & Bhattacharya, 2016), (Aghili et al., 2022), (Algani et al., 2022), (Alwadain & Ali, 2023), (Binsawad, 2025), (Btoush et al., 2025), (Dichev & Zarkova, 2025), (Latipov et al., 2025), (Mienye & Swart, 2024), (Mohammed et al., 2023), (Song et al., 2020), (Wu et al., 2025), (Zeng, 2021), (Zhu et al., 2025), (Zhou et al., 2019), (Zhang et al., 2020), (Mekterovi et al., 2021), (Aziz et al., 2022)

Specific (TNR)	Specificity = 1 – FP	(Charizanos et al., 2024), (Hilal et al., 2022), (Schneider & Brühl, 2023), (West & Bhattacharya, 2016), (Aghili et al., 2022), (Mienye & Swart, 2024), (Song et al., 2020)
AUC	AUC = area below the ROC curve	(Al-hashedi & Magalingam, 2021), Almazroi & Ayub, 2023), (Ashtiani & Rahemi, 2022), (Chen & Wu, 2023), (Hilal et al., 2022), (Li et al., 2024), (Lin, 2024), (Nassif et al., 2021), (Phua et al., 2016), (Schneider & Brühl, 2023), (Talukder et al., 2024), (West & Bhattacharya, 2016), (Aghili et al., 2022), (Alwadain & Ali, 2023), (Btoush et al., 2025), (Dichev & Zarkova, 2025), (Ekle & Eberle, 2025), (Mienye & Swart, 2024), (Mohammed et al., 2023), (Mytnyk et al., 2023), (Song et al., 2020), (Zeng, 2021), (Zhao & Bai, 2022), (Zhu et al., 2025), (Hamal & Senvar, 2021)

Model accuracy shows how much of the prediction is generated according to actual conditions (Ashtiani & Rahemi, 2022) (Wu et al., 2025). Meanwhile, precision measures the degree of accuracy of positive predictions made by the model (Hilal et al., 2022), (Lin, 2024), (Mim et al., 2024), (Nassif et al., 2021). Positive detection rate, or sensitivity (*remember*), shows how well the model is able to correctly recognize positive data (West & Bhattacharya, 2016), (Aghili et al., 2022). Specificity is the ratio between the number of correct negative predictions and the overall negative data (Mohammed et al., 2023), (Song et al., 2020), (Wu et al., 2025). Despite the precision and *remember* Equally important, the two have opposite relationships. Increased value *remember* generally will lead to a decrease in precision value, and vice versa. To balance the two metrics, F1 score is used, which is the harmonic mean between precision and *remember* (Talukder et al., 2024). F1 *Score* It is considered a better size because it is able to reflect the balance between precision and *remember.* To understand the impact of decision threshold changes on precision values and *remember*, used a parametric evaluation approach (Latipov et al., 2025), (Mienye & Swart, 2024). The goal is to maximize classification performance by optimally adjusting the classification threshold.

Other metrics include *Receiver Operating Characteristics* (ROC) *Precision Pulling Curves and Curves* (Al-hashedi & Magalingam, 2021). The value on the ROC curve is measured using *Areas below the curve* (AUC), which indicates the performance of the classification model (Hilal et al., 2022). A perfect model has an AUC value of 1, while a random model approaches an AUC value of 0.5. Some research from (Zhu et al., 2025), (Hamal & Senvar, 2021) Other metrics include *Average squared error* (MSE), *Euclidean Distance*and *Manhattan Distance*, which is commonly used in clustering methods to measure the degree of similarity or difference between data. These metrics are calculated based on the patterns and relevant features that the data has. Table 5 in this document presents the performance evaluation formula, along with its explanation and the amount of data used for each metric. As for the FPR metric (*false positive rate*) and FNR (*False negative rate*), the lower the value, the better the model's generalization ability to new data. In the table, TP, TN, FP, and FN refer to the *True positives*, *True negatives*, *False positives*and *False negatives*.

Compared tp earlier systematic reviews (Hilal et al., 2022), (Nassif et al., 2021) and (Aziz et al., 2022) thi study contributes a broader analytical lens by connecting ML algorithms, fraud domains, and evaluation metrics in one comprehensive synthesis. It not only identifies dominant thecniques bot also duscusses the interplay between methodological choces, dataset composition, and accuracy outcomes.

This studi provides a conceptual framework illustrating how data preprocessing, algorithmic selection, and model evaluation influence the detection of different fraud types. By systematically classifying findings from the last decade, it fills a research gap in understanding the comparative efficiency of ML methods in financial fraud detection.

CONCLUSION AND RECOMMENDATIONS

Financial fraud can occur in various sectors such as insurance, banking, taxation, and the corporate sector (Hilal et al., 2022). In recent years, the issue of financial fraud has become increasingly a serious concern among companies and industries. Although various efforts have been made to eradicate this fraudulent practice, its existence still continues and has a negative impact on the economy and society, because huge financial losses occur every day (Tubb et al., 2018). With progress *Artificial Intelligence* (AI), *Machine Learning* (ML) can now be appropriately leveraged to detect suspicious financial transactions through the analysis of large amounts of data. In this study, a systematic review is presented that examines and summarizes the literature related to financial fraud detection based on *Machine Learning*. The study adopts the Kitchenham methodology which uses clear protocols to extract, synthesize, and report research results.

A total of 38 articles were selected after the inclusion selection process was carried out. From the results of the review, various *machine learning* techniques commonly used for fraud detection are presented, the most frequently studied types of fraud, and the evaluation metrics used. Based on the reviewed article, *the most commonly used machine learning* algorithms to detect fraud are *Logistic Regression, Support Vector Machine*, *K-Nearest Neighbors* Algorithm and *Random Forest* from Decision *Tree* development. Meanwhile, the most discussed type of fraud in the literature is *credit card fraud*. As well as the evaluation metrics *of Accuracy*, *F1-score*, and *Recal/Sensibility*. Which is widely used in *machine learning methods*.

This systematic literature review successfully identified *machine learning* and the types of fraud that are relevant in the detection of financial fraud. This study is designed to maintain validity, but it still has some limitations, namely, it only includes journal articles and proceedings, without taking into account other sources such as reference books, the potential for missing literature from digital libraries that are not accessed or due to the variety of search terms and restrictions on English-language articles, which could make studies in other languages unaffordable.

This study contributes theoretically by mapping the intersection of fraud types, ML algorithms, and performance metrics, forming a unifies framework for understanding fraud detection research. Practically it provides insights for researchers, financial institutions, and policymakers to select, design, and implement more robust and adaptive detection systems. Future studies are encouraged to focu on: explainable AI (XAI) model that enhance interpretability and transparency in dicision making real time adaptive learning systems capable of responding to evolving fraud behaviors, And meta analysis methods to statistically measure the effect size of ML algorithms and strengthen empirical conclusions. Througt these directions, subsequent research can continue refining ML based fraud detection to be not only accurate but also ethical, transparent, and adaptable to emerging financial challenges.

REFERENCES

Aghili, S. N., Rasekh, M., Karami, H., Azizi, V., & Gancarz, M. (2022). Detection of fraud in sesame oil with the help of artificial intelligence combined with chemometrics methods and chemical compounds characterization by gas chromatography – mass spectrometry. *LWT*, *167*(July).

Ahmed, R., & Alrasheed, R. (2025). Building Public Trust in Bahrain : Leveraging Artificial Intelligence to Combat Financial Fraud and Terrorist Financing Through Cryptocurrency Tracking. *Social Sciences MDPI*, *14*(308).

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

Alamri, M., & Ykhlef, M. (2024). Hybrid Undersampling and Oversampling for Handling Imbalanced Credit Card Data. *IEEE Access*, *12*(January), 14050–14060. https://doi.org/10.1109/ACCESS.2024.3357091

Algani, Y. M. A., Vinodhini, G. A. F., Isabels, K. R., Kaur, C., Treve, M., Bala, B. K., Balaji, S., & Devi, G. U. (2022). Analyze the anomalous behavior of wireless networking using the big data analytics. *Measurement: Sensors*, *23*(August), 100407. https://doi.org/10.1016/j.measen.2022.100407

Almazroi, A. A., & Ayub, N. (2023). Online Payment Fraud Detection Model Using Machine Learning Techniques. *IEEE Access*, *11*(December), 137188–137203. https://doi.org/10.1109/ACCESS.2023.3339226

Alwadain, A., & Ali, R. F. (2023). Estimating Financial Fraud through Transaction-Level Features and Machine Learning. *Marhematics MDPI*, *11*(184).

Ashtiani, M. N., & Raahemi, B. (2022). Intelligent Fraud Detection in Financial Statements Using Machine Learning and Data Mining : A Systematic Literature Review. *IEEE Access*, *10*(July), 72504–72525. https://doi.org/10.1109/ACCESS.2021.3096799

Aziz, R. M., Baluch, M. F., Patel, S., & Kumar, P. (2022). A Machine Learning based Approach to Detect the Ethereum Fraud Transactions with Limited Attributes A Machine Learning based Approach to Detect the Ethereum Fraud Transactions with Limited Attributes. *Karbala International Journal of Modern Science 8*, *8*(2).

Binsawad, M. (2025). Enhanced Financial Fraud Detection Using an Adaptive Voted Perceptron Model with Optimized Learning and Error Reduction. *Electronics MDPI*, *14*(1875).

Btoush, E., Zhou, X., Gururajan, R., & Chan, K. C. (2025). Achieving Excellence in Cyber Fraud Detection : A Hybrid ML + DL Ensemble Approach for Credit Cards. *Applied Sciences*, *15*.

Chaquet-ulldemolins, J., Moral-rubio, S., & Muñoz-romero, S. (2022). On the Black-Box Challenge for Fraud Detection Using Machine Learning (II): Nonlinear Analysis through Interpretable Autoencoders. *Applied Sciences*, *Ii*.

Charizanos, G., Demirhan, H., & İçen, D. (2024). An online fuzzy fraud detection framework for credit card transactions. *Expert Systems With Applications*, *252*. https://doi.org/10.1016/j.eswa.2024.124127

Chen, Y., & Wu, Z. (2023). Financial Fraud Detection of Listed Companies in China : A Machine Learning Approach. *Sustainability MDPI*, *15*.

Chithanuru, V., & Ramaiah, M. (2025). Proactive detection of anomalous behavior in Ethereum accounts using XAI-enabled ensemble stacking with Bayesian optimization. *PeerJ Computer Science*. https://doi.org/10.7717/peerj-cs.2630

Delamaire, L., Abdou, H. A., & Pointon, J. (2019). Credit card fraud and detection techniques : a review. *Banks and Bank Systems*, *4*(2).

Dichev, A., & Zarkova, S. (2025). Machine Learning as a Tool for Assessment and Management of Fraud Risk in Banking Transactions. *Journal of Risk and Financial Management*, *18*(130).

Ekle, O. A., & Eberle, W. (2025). Adaptive DecayRank : Real-Time Anomaly Detection in Dynamic Graphs with Bayesian PageRank Updates. *Applied Sciences*, 1–24.

Faraji, Z. (2022). A Review of Machine Learning Applications for Credit Card Fraud Detection

with A Case study. *Journal of Management*, *5*(1), 49–59.

Firdaus, R., Xue, Y., Gang, L., Sibt, M., & Bari, P. (2022). Artificial Intelligence and Human Psychology in Online Transaction Fraud. *Frontiers in Psychology*, *13*(October), 1–9. https://doi.org/10.3389/fpsyg.2022.947234

Gyamfi, N. K. (2018). Bank Fraud Detection Using Support Vector Machine. *In Proceedings of the 2018 IEEE 9th Annual Infor Mation Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC*, 37–41. https://doi.org/10.1109/IEMCON.2018.8614994

Hamal, S., & Senvar, O. (2021). *Comparing performances and effectiveness of machine learning classifiers in detecting financial accounting fraud for Turkish SMEs*. *14*(1), 769–782.

Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial Fraud : A Review of Anomaly Detection Techniques and Recent Advances. *Expert Systems With Applications*, *193*, 116429. https://doi.org/10.1016/j.eswa.2021.116429

Isong, B. E., & Bekele, E. (2013). A Systematic Review of Fault Tolerance in Mobile Agents. *American Journal of Software Engineering and Applications*, *January*. https://doi.org/10.11648/j.ajsea.20130205.11

Kanika, Singla, J., Bashir, A. K., Nam, Y., Hasan, N. U. I., & Tariq, U. (2022). Handling Class Imbalance in Online Transaction Fraud Detection. *Computers, Materials & Continua*, *70*(2). https://doi.org/10.32604/cmc.2022.019990

Kitchenham, B., & Charters, S. M. (2007). *Guidelines for performing Systematic Literature Reviews in Software Engineering Guidelines for performing Systematic Literature Reviews in Software Engineering*. *October*.

Latipov, Z. A., Naminova, K. A., Abdullayev, I. S., Ilyin, A. E., Shichiyakh, R. A., & Lydia, E. L. (2025). Optimizing Financial Fraud Detection : Understandings from Variable Selection with Neutrosophic Vague Soft Set. *International Journal of Neutrosophic Science*, *25*(03), 219–230.

Lee, K. (2018). An Artificial Intelligence Approach to Financial Fraud Detection under IoT Environment : A Survey and Implementation. *Security and Communication Networks*, *2018*.

Li, B., Yen, J., & Wang, S. (2024). Uncovering Financial Statement Fraud : A Machine Learning Approach With Key Financial Indicators and Real-World Applications. *IEEE Access*, *12*(November), 194859–194870. https://doi.org/10.1109/ACCESS.2024.3520249

Lin, D. (2024). Key Considerations to be Applied While Leveraging Machine Learning for Financial Statement Fraud Detection : A Review. *IEEE Access*, *12*(November), 168213–168228. https://doi.org/10.1109/ACCESS.2024.3488832

Mekterovi, I., Karan, M., Pintar, D., & Brkic, L. (2021). applied sciences Credit Card Fraud Detection in Card-Not-Present Transactions : Where to Invest ? *Applied Sciences*, *11*(6766).

Mienye, I. D., & Swart, T. (2024). A Hybrid Deep Learning Approach with Generative Adversarial Network for Credit Card Fraud Detection. *Technologies MDPI*, *12*(186).

Mim, M. A., Majadi, N., & Mazumder, P. (2024). Heliyon A soft voting ensemble learning approach for credit card fraud detection. *Heliyon*, *10*(3), e25466. https://doi.org/10.1016/j.heliyon.2024.e25466

Mohammed, M. A., Boujelben, M., & Abid, M. (2023). A Novel Approach for Fraud Detection in Blockchain-Based Healthcare Networks Using Machine Learning. *Future Internet MDPI*, *15*.

Mytnyk, B., Tkachyk, O., Shakhovska, N., & Fedushko, S. (2023). Application of Artificial Intelligence for Fraudulent Banking Operations Recognition. *Big Data and Cognitive*

Computing, *7*.

Nassif, A. B., Talib, M. A., Nasir, Q., & Dakalbab, F. M. (2021). Machine Learning for Anomaly Detection : A Systematic Review. *IEEE Access*. https://doi.org/10.1109/ACCESS.2021.3083060

Page, M. J., Mckenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-wilson, E., Mcdonald, S., … Moher, D. (2021). The PRISMA 2020 statement : an updated guideline for reporting systematic reviews Systematic reviews and Meta-Analyses. *Research Methods & Reporting*. https://doi.org/10.1136/bmj.n71

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

Phua, C., Lee, V., Smith, K., & Gayler, R. (2016). A Comprehensive Survey of Data Mining-based Fraud Detection Research. *Comput. Secur*, *57*, 47–66.

Qiu, S., & He, H. (2018). Machine Learning- and Evidence Theory-Based Fraud Risk Assessment of China ' s Box Office. *IEEE Access*, *6*, 75619–75628. https://doi.org/10.1109/ACCESS.2018.2883487

Randhawa, K., Loo, C. K., Seera, M., Lim, C. P., & Nandi, A. K. (2018). Credit Card Fraud Detection Using AdaBoost and Majority Voting. *IEEE Access*, *6*(February), 14277–14284. https://doi.org/10.1109/ACCESS.2018.2806420

Rb, A., & Kr, S. K. (2021). Credit card fraud detection using artificial neural network. *Global Transitions Proceedings*, *2*(1), 35–41. https://doi.org/10.1016/j.gltp.2021.01.006

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

Saleh, M. M. A., Aladwan, M., Alsinglawi, O., & Almari, mohammad O. S. (2021). PREDICTING FRAUDULENT FINANCIAL STATEMENTS USING FRAUD DETECTION MODELS. *Academy of Strategic Management*, *20*(3), 1–17. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.abacademies.org/articles/Predicting-fraudulent-financial-statements-using-fraud-detection-models-1939-6104-20-S3-002.pdf

Schneider, M., & Brühl, R. (2023). Disentangling the black box around CEO and financial information - based accounting fraud detection : machine learning - based evidence from publicly listed U . S . firms. In *Journal of Business Economics* (Vol. 93, Issue 9). Springer Berlin Heidelberg. https://doi.org/10.1007/s11573-023-01136-w

Song, R., Huang, L., Cui, W., & Vanthienen, J. (2020). applied sciences Fraud Detection of Bulk Cargo Theft in Port Using Bayesian Network Models. *Applied Sciences*, *10*, 1–22.

Talukder, A., Khalid, M., & Uddin, A. (2024). An integrated multistage ensemble machine learning model for fraudulent transaction detection. *Journal of Big Data*. https://doi.org/10.1186/s40537-024-00996-5

Tubb, N. F. R., Krause, P., & Garn, W. (2018). How Artificial Intelligence and machine learning research impacts payment card fraud detection: Asurvey and industry benchmark. *Engineering Applications of Artificial Intelligence*, *76*, 130–157.

Usman, A. U., Abdullahi, S. B., Rehman, A., & Member, S. (2024). Financial Fraud Detection Using Value-at-Risk With Machine Learning in Skewed Data. *IEEE Access*, *12*(May), 64285–64299. https://doi.org/10.1109/ACCESS.2024.3393154

West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection : A comprehensive review. *Computers & Security*, *57*, 47–66. https://doi.org/10.1016/j.cose.2015.09.005

Wu, Y., Wang, L., Li, H., & Liu, J. (2025). A Deep Learning Method of Credit Card Fraud

Detection Based on Continuous-Coupled Neural Networks. *Mathematics*, *13*, 1–18.

Zeng, Y. (2021). RLC-GNN : An Improved Deep Architecture for Spatial-Based Graph Neural Network with Application to Fraud Detection. *Applied Sciences*.

Zhang, Z., Chen, L., Liu, Q., & Wang, P. (2020). A Fraud Detection Method for Low-Frequency Transaction. *IEEE Access*, *8*.

Zhao, Z., & Bai, T. (2022). Using SMOTE and Machine Learning Algorithms. *Entropy MDPI*, *24*(1157), 1–17.

Zhou, H., Sun, G., Fu, S., Jiang, W., & Xue, J. (2019). *A Scalable Approach for Fraud Detection in Online E-Commerce Transactions with Big Data Analytics*. *60*(1), 179–192. https://doi.org/10.32604/cmc.2019.05214

Zhu, S., Ma, T., Wu, H., Ren, J., He, D., & Li, Y. (2025). Expanding and Interpreting Financial Statement Fraud Detection Using Supply Chain Knowledge Graphs. *Journal of Theoretical and Applied Electronic Commerce Researh MDPI*, *20*(26), 1–19.