
WWJMRD 2024; 10(02): 43-53
www.wwjmrd.com
*International Journal*
*Peer Reviewed Journal*
*Refereed Journal*
*Indexed Journal*
*Impact Factor SJIF 2017: 5.182 2018: 5.51, (ISI) 2020-2021: 1.361*
*E-ISSN: 2454-6615*

**Bertha C. Ori**
Kingsley Ozumba Mbadiwe University, Imo State Nigeria.

**Cletus I. Ori**
Wrexham University, United Kingdom.

**Lilian O. Ezekiel**
43 Crescent, Salford, M5 4WT.

**Correspondence**:
**Bertha C. Ori**
Kingsley Ozumba Mbadiwe University, Imo State Nigeria.

# Exploring Financial Fraud Detection: A Comprehensive Analysis and Implementation of Machine Learning with Artificial Neural Networks

**Bertha C. Ori, Cletus I. Ori, Lilian O. Ezekiel**

**Abstract**
Financial fraud, characterized as deceptive strategies aimed at securing financial gains, has emerged as a widespread threat to companies and organizations worldwide. Traditional methods like manual verifications and inspections are not only imprecise but also incur high costs and time consumption in identifying fraudulent activities. The rise of artificial intelligence has paved the way for intelligent machine learning approaches to efficiently detect fraudulent transactions through the analysis of extensive financial data. This paper seeks to offer a systematic literature review (SLR) that methodically examines and consolidates existing literature on machine learning (ML)-based fraud detection. To conduct this review, the artificial neural network approach was employed to demonstrate fraud detection procedure with 70 % of sample data for training, 15% for testing and 15% for validation. Numerous studies were collected through specified search strategies from popular electronic database libraries. Following the application of inclusion/exclusion criteria, a considerable number of articles were thoroughly examined, synthesized, and analyzed. The review provides an overview of prevalent ML techniques employed in fraud detection, the most common type of fraud addressed, and the evaluation metrics utilized. The scrutinized articles revealed that support vector machine (SVM) and artificial neural network (ANN) are popular ML algorithms employed for fraud detection, with credit card fraud being the most frequently addressed fraud type using ML techniques. The paper concludes by highlighting key issues, identifying gaps, and delineating limitations in the field of financial fraud detection. Additionally, it suggests potential areas for future research in this domain.

**Keywords:** Financial fraud; fraud detection; machine learning; data mining; support vector machine (SVM), artificial neural network (ANN).

## 1. Introduction

Financial fraud involves the illicit pursuit of financial gains through illegal means [1,2]. This deceptive practice extends to various sectors, including insurance, banking, taxation, and corporate domains [3]. In recent times, the rise of financial transaction fraud [4], money laundering, and other forms of financial fraud [5] poses a growing challenge to companies and industries [4]. Despite concerted efforts to curb fraudulent activities, their persistence has adverse effects on the economy and society, resulting in substantial daily financial losses [6]. Numerous approaches to fraud detection have been introduced over the years [1]. However, traditional manual methods are not only time-consuming, expensive, and imprecise but also impractical [7]. Although studies aim to minimize losses from fraudulent activities, their efficiency remains limited [5]. The advent of artificial intelligence (AI) has led to the utilization of machine learning and data mining for the detection of fraudulent activities in the financial sector [8,9].Both unsupervised and supervised methods have been employed for predicting fraud activities[10], with classification methods emerging as the most popular for detecting fraudulent transactions.

This study seeks to identify machine-learning-based techniques for detecting financial transaction fraud and analyze existing gaps to uncover research trends in this field. While previous reviews have explored various aspects of fraudulent financial activities, other areas where AI and ML has been used explored is reported elsewhere [11–17], this study aims to provide a comprehensive overview that encompasses all popular areas of financial fraud activities, addressing a notable gap in the existing literature. Despite existing reviews in the field, many studies have focused on specific finance areas, such as credit card fraud [18], online banking fraud [19], bank credit administration fraud [20], and payment card fraud [21]. This study aims to fill this gap by presenting a broad examination of machine learning (ML)-based methods applied to financial transaction fraud detection. The systematic literature review (SLR) presented here aims to guide researchers in selecting ML-based financial transaction fraud detection methods and the corresponding datasets for predicting fraudulent activities in financial transactions. The remainder of this paper is organized as follows: Section 2 details review of research methodology, including search criteria, study selection, data extraction, and quality evaluation. Section 3 presents the SLR findings and responses to the study questions. The discussion and potential challenges impacting the validity of this review are addressed inSections 4 and 5, respectively. Finally, Section 6 provides a conclusion for the study.

## 2. ResearchMethodologyReview

This paper employs a Systematic Literature Review (SLR) approach, a thorough method for collecting and analyzing studies that address specific research questions [22]. SLR approach is chosen to aggregate and synthesize information pertaining to particular issues, aiming to reduce biases[22]. It aims to deliver are view with high-quality evidence while scrutinizing the rationale behind reviewers' judgments and conclusions [22]. The methodology of this SLR study is derived from the framework presented in a prior study [23], encompassing three primary stages: review planning, conducting the review, and reporting the review. The key stages of the SLR process are visually depicted in Figure 1.

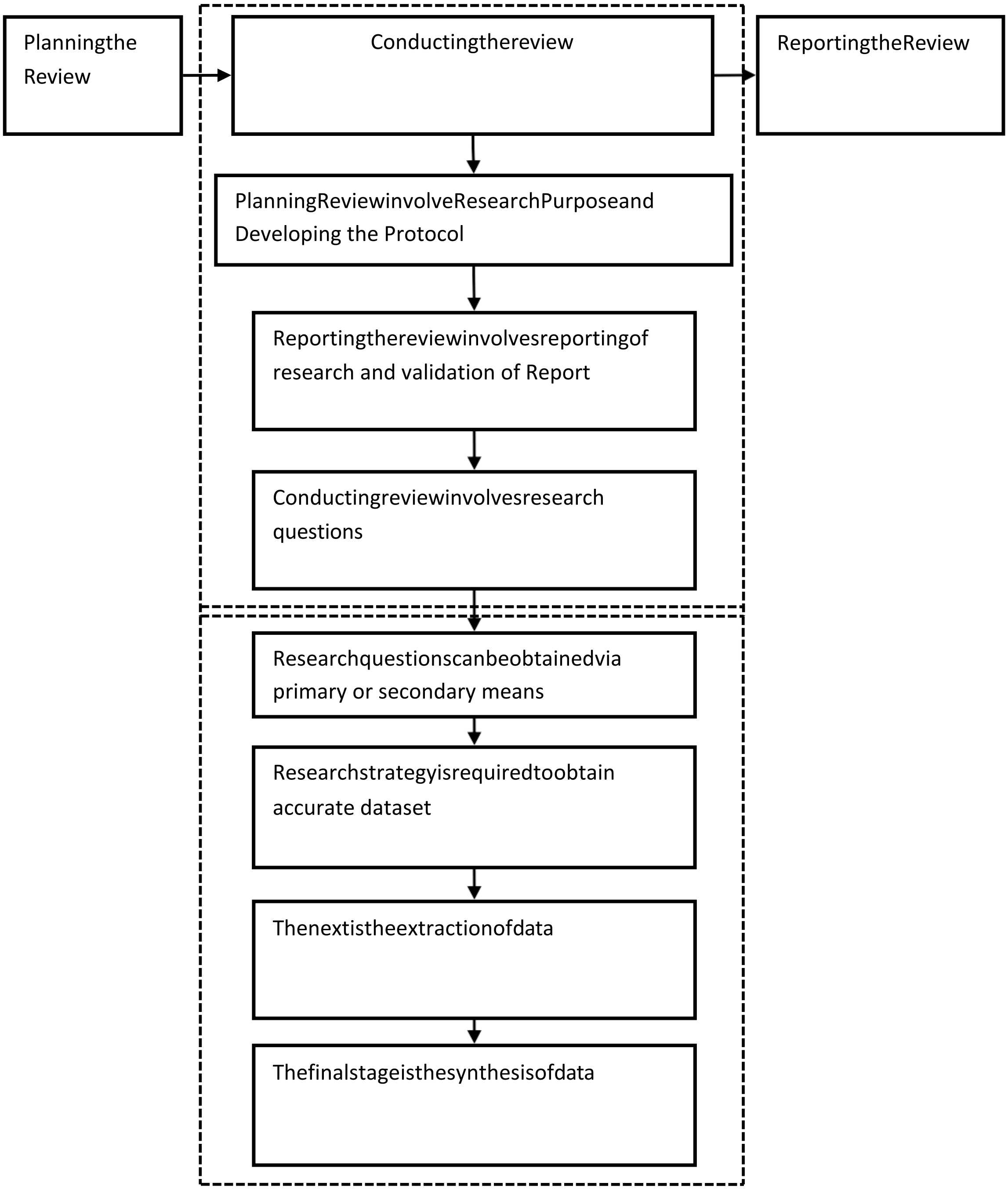


**Figure1**StagesoftheSLR

Review Planning

Objective of the Review: The purpose of the review, such as understanding the current state of research on detecting financial fraud through machine learning is significant. Scope and Inclusion/Exclusion Criteria: It is important to define the criteria for including or excluding studies. For example, you might specify the publication date range, types of studies (e.g., empirical studies, case studies), and the focus on machine learning methods for fraud detection. The planning stage encompasses the preparatory and developmental processes of the Systematic Literature Review (SLR), involving the identification of the research goal and the formulation of the review protocol [24]. To retrieve more relevant papers, an automated search was conducted on major digital databases [25,26]. Other similar databases were not considered; as primary sources' index data were deemed sufficient. The selection of these libraries was based on their popularity and status as rich sources of articles pertinent to the research questions addressed in this study. To ensure a comprehensive and current review, the time frame for considerations pans till 2021. Following the planning phase, the subsequent stage involves conducting the review. This step constitutes the primary review process, encompassing the identification of the research questions for the review, outlining the key issues to be discussed and analysed. This stage includes the selection of the search strategy and the procedures for data extraction and synthesis, elaborated in the following subsections:

Research Questions

In the initial phase of this review, the crucial task involves formulating research questions to precisely pinpoint the issues under scrutiny. This process is fundamental in determining the key studies to be incorporated into there view, making the formulation of research questions a central aspect of the SLR. Table 1 provides an overview of the primary Research Questions (RQs) employed in this study. The primary aim of the first question is to identify prevalent categories of financial fraud addressed through the application of machine learning (ML) methods. The second question is focused on identifying commonly used ML approaches for the detection of fraudulent financial activities. The third and fourth questions are crafted to delineate the performance evaluation metrics utilized in ML-based financial fraud detection and to uncover research gaps, trends, then a brief demonstration of fraud detection by implementing Neural Network and finally, future directions in this field.

Search Strategy

This is focused more on the approach to be used to search for relevant literature. The process has to do with detailing plan for searching and selecting studies for the review. This section provides a clear and reproducible process. This includes databases, keywords, search filtered. Databases: Specify the databases you plan to search. This could include academic databases (e.g., PubMed, IEEE Xplore, ScienceDirect) and any specialized databases related to finance or machine learning.

Keywords and Search Terms: List the keywords and search terms you will use to identify relevant studies. Consider using variations and synonyms to ensure a comprehensive search.

Search Filters: Inapplicable, mention any filters or criteria you will apply during the search(e.g., language, publication date).

Search Timeline: Provide information on when you conducted or plan to conduct the search to make it clear that the review is based on the most current literature. Remember to follow best practices for the reviews to ensure transparency and reproducibility. It's also essential to document any deviations from the planned protocol and justify them in the final review.

Study Selection Criteria

Follow Ing the appl cation of the search terms across the mention digital libraries, recent papers were identified and subsequently filtered. After eliminating duplicates, the selection process continued with standard articles. The authors established inclusion and exclusion criteria during the search process to identify the most relevant papers, screening these studies according to quality assessment standards to ensure their reliability.

**3.** Search Results and Meta-Analysis: This section presents the search results obtained from the second stage of the review process, which involves selecting the relevant studies to be considered in this SLR study. It is important to present the description of the reviewed studies in this SLR and answer each of the research questions specified in the section.

Description of Studies

The number of articles relating to financial fraud detection using ML approaches which provides a chronological summary of the published articles is considered.

Synthesis Results

This section unveils the outcomes of the data synthesis aimed at addressing the research questions derived from the selected papers. Herein, the designed research questions for the Systematic Literature Review (SLR) will be addressed.

ResearchQuestion1:

What are the different categories of fraudulent activities that are addressed using ML techniques?

Fraudulent activities exhibit variations across industry sectors [27]. This section responds to researchquestion1 by delineating various fraudulent activities addressed through the application of machine learning (ML) techniques based on the selected articles. According to the reviewed literature, fraudulent activities in the financial sector can be broadly categorized into credit card, mortgage, financial statement, and health care fraud.

(a) Credit Card Fraud

Credits typically refer to electronic financial transactions conducted without the use of physical cash[28]. Accredit card, commonly used for online transactions, is a small piece comprising thin plastic material containing credit services and customer details [28–30]. Fraudsters exploit credit cards for unlawful transactions, resulting in significant losses for both banks and cardholders [31]. The creation of counterfeit cards has facilitated easier execution of illicit transactions. Unauthorized use of the card, obtained illegitimately, deems any ensuing transaction as fraudulent [29]. Credit card fraudulent activities encompass offline and online fraud. In offline fraud, perpetrators execute illicit transactions with stolen credit cards, resembling genuine cardholders, while online fraud occurs during Internet transactions [30].

(b) Financial Statement Fraud

Fraud in financial statements involves manipulating financial reports to falsely depict a company as more profitable than actual, thereby evading taxes, inflating stock prices, or securing bank loans [31,32]. These statements comprise confidential records containing financial information, expenses, profits, income, loans, and management write-ups discussing business performances and future trends [33–37]. Financial statement fraud aims to enhance share prices, reduce tax liabilities, attract investors, and secure personal bank loans [15].

(c) Insurance Fraud

Insurance fraud entails the misuse of an insurance policy to gain illegitimate benefits from an insurance company [38]. Insurance, designed to protect transactions against financial risks, is particularly targeted in sectors such as healthcare and automobile insurance companies [39,40] with occasional instances in home and crop insurance. The estimated annual cost of insurance fraud in the United States exceeds a billion USD, eventually passed on to consumers through increased insurance premiums. Fraudulent claims in automobile insurance often involve deception during the claims process, ranging from individual fraudsters to organized groups staging or faking incidents [41–44]. Healthcare insurance fraud, a serious issue in contemporary society, is entwined with social, political, and economic concerns, incurring significant expenses associated with high-quality medical services.

(d) Financially-Fraud

Financial cyber fraud refers to crimes committed over cyberspace solely for illegal economic gain[45-46]. Perpetrators of financial cybercrime deliberately mask their activities to blend with normal online behavior. As criminals gain access to advanced technology, combating their tactics becomes increasingly challenging. This intersection of financial crime and cybersecurity has prompted financial institutions to develop in-house methods, including real-time analytics and interdiction tools, to protect assets and prevent financial loss. However, Alexis ting models exhibit signs of inadequacy in addressing these attacks, new methods incorporating machine learning and deep learning models are being explored [47–50].

(5) Other Financial Fraudulent Types

Beyond the mentioned types of fraudulent activities in the financial sector, additional frauds are prevalent, encompassing commodities and securities fraud, mortgage fraud, corporate fraud, and money laundering. Securities and commodities fraud occurs when individuals invest in companies based on false information. Mortgage fraud involves intentional misstatements made by debtors during application processes, targeting mortgage-related documents. Corporate fraud entails insiders falsifying financial documents to conceal fraud or criminal activities. Money laundering involves changing the source of illegal money to legitimize it, impacting society by facilitating other crimes suchas funding terrorism. Cryptocurrency fraud systematically deceives users with false investments, promising significant gains.

ResearchQuestion2:

What Arethe ML-Based Techniques for Financial Fraud Detection Employe din the literature?

Machine learning (ML) denotes analytical techniques that identify specific patterns without requiring manual guidance from inexpert [87]. Numerous researchers have extensively explored the application of ML methods in financial fraud detection. These methods encompass Support Vector Machine (SVM), Artificial Neural Network (ANN), Hidden Markov Model (HMM), k- Nearest Neighbors (KNN), Decision Tree, and more. Thus, to address the aforementioned research question (RQ2), this section outlines various popular ML methods utilized for financial fraud detection based on the selected articles in the review. A detailed explanation of the ML techniques employed in detecting financial fraudulent activities is presented in the following subsection.

(a) Fuzzy-Logic-Based Method

Fuzzy logic (FL) serves as an effective conceptual framework for addressing data representation in contexts of uncertainty and ambiguity [69]. This logical approach acknowledges that methods of thinking are estimations rather than precise. Fuzzy combinations offer effective concepts for handling complex modeling in innovative ways [52]. Multiple FL-based methods have been employed for fraud detection. An example is the FUZ-ZGY hybrid model, introduced in [69], designed to detect anomalous behaviors in credit card transactions. This model, grounded in fuzzy and Fogg behavioral concepts, employed fuzzy logic to track the historical activities of merchants and the Fogg behavioral method to characterize customer behavior along dimensions of fraud-committing ability and motivation. Another fuzzy-based method, presented in [68], aimedtodetectcreditcardfraudbycategorizingtransactionsinto fraudandnon-fraudcategories with reduced false positives. This method utilized fuzzy c-means clustering and an Artificial Neural Network (ANN) model, demonstrating efficacy on synthetic data with reduced false positives. Another study [69] proposed a fuzzy logic-based fraud detection method in the banking system, improving accuracy in classifying fraudulent and non-fraudulent activities in banking transactions by defining rules based on expert experience. This approach was further refined in [52], constructing fuzzy rules using fuzzy logic to enhance the detection of fraud transactions. [61] introduced a rule-based technique utilizing a firefly algorithm and threshold- accepting method to distinguish between fraudulent and non-fraudulent transactions based on financial activities. Additionally, [62] designed a fuzzy-rule-based approach for detecting financial fraud, integrating a rule-based approach with genetic feature selections to achieve good performance through feature selection and fuzzy unordered rule induction.

(a) Artificial Neural Network (ANN)

Artificial Neural Network (ANN) is an information-processing technique inspired by the behavior of biological neural networks [76]. ANN is particularly powerful when dealing with large volumes of data [88]. Several ANN-based methods have been proposed for fraudulent detection in the financial sector. Srivastava et al. [30] investigated credit card fraud detection on the trader's side using an ANN-based method that connects the merchant with payment gateways. Ghobadi and Rohani [77] developed a hybrid model based on a Cost-Sensitive Neural Network to identify credit card fraud, demonstrating increased detection rates and reduced false negative costs. Randhawa et al. [28] proposed research for discovering fraud in credit card transactions based on ML methods, including ANN models. An approach based on NN was introduced in [76] for detecting fraudulent transactions in credit cards, aiming to enhance the security and accuracy of automatic credit card transactions. Ravisankar et al. [33] introduced financial fraud detection using a Multilayer Feedforward Neural Network (MLFF).

(b) Support Vector Machine (SVM)

(b) SVM, a supervised ML method, aims to find maximum margin hyperplane for classifying input training data into two categories [41,66]. It possesses the capability to classify new data points based ona labeled training set for each class [68]. The literature review reveals several instances where researchers explored SVM techniques for fraud detection [65,66,80]. For instance, Rajak and Mathai [65] introduce dihybrid technique combining SV Mand the fusion Danger theory for fraudulent detection. The experimental results demonstrated that this approach outperformed existing methods in term so timebomb laxity and F-measure. In another study, Francis et al. [80] utilized the SVM technique to propose fraud detection by investigating an automated medical bill architecture. This research aimed to provide a swift response for detecting medical fraud in real time, with experimental results indicating superior performance compared to previous approaches. Additionally, Xu and Liu [66] applied optimized SVMto detect fraudulent activities in online credit card transactions. Hidden Markov Model (HMM)

The Hidden Markov Model (HMM) is a dual embedded random method commonly employed for handling more complex random processes compared to traditional Markov models [19]. Numerous methods in the reviewed literature have utilized the HMM technique for financial fraud detection. Agrawal et al. [19] introduced a hybrid method by integrating HMM and Genetic Algorithms (GA) for identifying credit card fraudulent transactions. This approach employed HMM to preserve previous transaction logs and GA to com pute the threshold value for clustering incoming transactions in to various clusters. The authors demonstrated that this method is more effective for credit card fraud detection. A similar approach was proposed in [86] for internet banking fraud detection by revealing legitimate users and monitoring their illicit behaviors. Another method in [73] utilized HMM to address limitations in existing fraud- detection methods during credit card operations. The studyfindingssuggestedthat HMMhasthe capability to enhance fraud detection and minimize false-positive rates. A comparable approach in[20] employedanHMM-basedtechniqueto enhancetheefficiencyandaccuracyofcredit card fraud detection, utilizing the clustering technique based onthe K-means methodto determine the clusters' closest centroids and integrate them into a single group.

(c) K-NearestNeighborsAlgorithm(KNN)

The K-Nearest Neighbors (KNN) algorithm is a convenient and straightforward supervised ML technique capable of addressing both regression and classic fiction processes [62].The class label in the KNN model is typically determined by using a small set of the nearest samples. This non- parametric model is used for both classification and regression tasks, identifying similar neighborhoods closest to a given sample point in dataset and creating new sample point based on the distance between two samples of data [70]. While KNN has demonstrated effectivenessonmanydatasets, its performance may be compromised by unbalanced datasets [78]. Malini and Pushpa [70] proposed a credit card detection approach using two methods: the KNN model and the outlier detection model. Experimental results indicated that the KNN models more effective for fraudulent detection in credit cards. Awoyemi et al. [78] utilized the KNN algorithm to investigate credit card transactions for detecting fraudulent behaviors, employing a credit card dataset proposed by cardholders. The finding demonstrated that the K-Nearest Neighbor performed.

(d) K-Nearest Neighbors Algorithm (KNN)

Badrinath al. [84] introduced unapproachable on the K-Nearest Neighbors (KNN) algorithm for auto insurance fraud detection, incorporating three methods: distance-based, density-based, and interquartile range within car insurance data. This work considers the influence of feature selection methods on accuracy scores. Similar methods were presented in [72] for detecting an omalous fraudulent transactions by integrating the KNN technique with Chi-Square Automatic Interaction Detection (CHAID) to enhance the performance of identifying fraudulent transactions.

(a) Bayesian Method

The Bayesian model (BN) is a specific type of graphical model that considers both independent and conditional relationships between various variables. BN uses nodes and edges in a directed graph to represent these relationships and is particularly adept at conducting anonymous probability computations [56]. In their viewed literature, weexplored various papers focusing on two main types of Bayesian methods: the Bayesian belief network and Naive Bayes (NB). NB is an ML model based on Bayes' theorem, predicting membership probabilities for each class. It forecasts the label of a given data point based on the probability of belonging to a specific category [56]. The results in a study demonstrated the effectiveness of the proposed model in fraud detection. Richter and Herland [81] utilized the NB algorithm to address fraudulent transactions in the health sector based on medical procedure records. The research aimed to classify supplier behavior regarding whether it is anomalous or not. To enhance fraud detection, Hajek and Henriques [33] proposed an intelligent method for detecting fraudulent financial documents by extracting specific features from financial reports.

(b) DecisionTree(DT)

A decision tree (DT) is an ML technique employed to construct decision support tools, representing binary options over features in inner nodes [69]. Numerous methods based on decisiontrees havebeenemployedforfinancialfrauddetectionovertheyears. DeviandKavitha [78] devised a DT-based method to categorize credit card transactions as normal or suspicious data, outperforming existing approaches with high accuracy. In the realmofau to fraud detection, a study [79] compared three methods—Naive Bayes (NB), DT, and Random Forest (RF)—with DT emerging as the superior performer. Kho and Vea [67] scrutinized credit cardholders' transaction behavior, differentiating between normal and abnormal transactions using ML algorithms such as Random Tree (RT) and NB, with RT demonstrating superior performance in evaluations on synthetic datasets. A comparable approach was implemented in [42] to detect fraud in the auto insurance sector, utilizing an adaptive oversampling method to address imbalanced classes in insurance datasets.

(c) Genetic Algorithm (GA)

The genetic algorithm (GA), inspired by natural evolution, utilizes binary strings known as chromosomes to search for optimal solutions [35]. Gupta and Gill [35] employed GA for financial fraud detection in companies. Benghazi et al. [71] introduced a novel technique for fraud detection in credit card transactions, addressing issues in detecting minority class objects in imbalanced datasets by combining K-means and GA. The K-means method was initially used to group and classifyminorityinstances, followed by the application of GA to create new instances with easyGroup, for minga new training data set. Özçeliketal.[61] also utilized GA to address problems related to detecting fraudulent credit card transactions in a real-world application project.

(e) Ensemble Methods

Ensemble methods, meta-algorithms that combine various intelligent techniques into a single predictive approach, aim to mitigate weaknesses in individual models by leveraging stronger models [33]. Different ensemble techniques serve diverse purposes, such as boosting to reduce bias, bagging to decrease variance, and stacking to enhance predictions [33]. Among the ensemble methods, random forest (RF) stands out as the most commonly used in the literature [33].

(f) Random Forest(RF)

RF outputs the median prediction for regression tasks and the mode of classes for single trees in classification problems. Recent research has demonstrated that RF outperformed other comparative methods [64]. Bootstrap Aggregating (BA), commonly known as bagging, creates multiple samples fromtraining instances with replacements. Numerous studies in financial fraud detection have applied bagging techniques [33].

(k) Boosting

Boosting, which involves altering the distribution of the training dataset based on predecessor accuracy, aims to sequentially train weak learners [28]. Ad boost, a popular boosting technique, was employed in [28]. AdaboostMI, a multi-instance Adaboost, repetitively executes different SVM distributions throughout the training dataset and combines the classifiers into a distinct hybrid classifier [33].

(l) Stacking

Stacking, an ensemble ML method, combines various classification or regression models, using the entire dataset and typicallyemploying different models than those used in bagging [2].

(m) Clustering-BasedMethods

Clustering, an unsupervised learning method grouping similar instances, is popular in financial fraud detection, although it was less frequently implemented than classification techniques in reviewed articles [5]. Glancy and Yadav [56] utilized text-mining hierarchical clustering tocreate a financial transaction fraud-detection model, employing the SVDs technique for text dimension reduction. Another approach by Glancy and Yadav [56] used the dual GHSOM technique to detect non-fraud-centric spatial hypotheses, capturing the topological patterns of fraudulent financial transactions.

LR techniques are primarily employed in binary and multi-class classification problems [35,78]. Lroperatesbyconductingregressiononasetofvariablesandisparticularlyusefulfor describing patterns and elucidating connections between various dependent binary variables. Logistic regression is one of the most frequently utilized machine learning (ML) techniques for detecting financial misstatement models. The majority of studies, as indicated in that review, employed LR techniques for financial fraud detection. Peng and You [81] proposed an effective technique for identifying characteristics related to fraud lent transaction detection using LR after a comprehensive review of published data. The authors compared the predictive ability of their proposed method against other detection methods, with the ML techniques used for financial fraud detection.

**ResearchQuestion3:**

What are the Evaluation Metrics Utilized for Assessing Financial Fraud Detection through Machine Learning Methods

In the context of financial fraud detection, evaluating the performance of a model is crucial, as highlighted in prior research [38,40,84]. While there are no rigidly prescribed evaluation measures specifically designated for assessing machine learning (ML) techniques in fraud detection [38,72], recent studies have witnessed the application of various performance evaluation metrics by different researchers. These metrics encompass accuracy, precision, recall, F1 measure, false-negative rate (FNR), area under the curve (AUC), specificity, and more. The ensuing section provides an overview of the evaluation metrics employed in the scrutinized papers, with the formulas for different performance measures.

The model's accuracy quantifies the overall accuracy of the model's predictions, while precision assesses the accuracy of the model's positive predictions [42,69,82]. Recall, also known as sensitivity, gauges the percentage ofpositive cases accurately identified bythe classifier [21,67]. The next section is a demonstration of the ANN model for fraud detection.

## 4. Application Using Arti facial Neural Network (ANN)Model

A simulation of the Neural Network Model for identifying financial fraud via an ArtificialNeural Network (ANN) involves a parametric examination, where the dataset obtained from a financial institution is divided into training, testing, and validation sets. Specifically, 70% of the dataset is designated for training, 15% for testing, and an additional 15% for validation. In the graphical representation (see Fig. 2), the straight lines portray the linear relationships betweenthe output and the target data employed in this study. The correlation coefficients (R) betweenthe actual and predicted values are as follows: 0.99966 for the training set, 0.93928 for the validation set, 0.90388 for the testing set, and 0.74523 for overall performance. The determinationcoefficient (R2) for the entire network is computed as 0.856. The notablyelevated correlation coefficients observed in the training, validation, and testing phases underscore the model's precision in prediction. The average determination coefficient (R2 = 0.856) indicatesthatapproximately 86%of thedatawaseffectively utilizedforpredictivepurposes.Thisvalue signifiescommendableperformanceintherealmoffinancialfrauddetectionusingtheANN Model.

## 5. AnalysisoftheStudy

ValidationandTestinginANNfor Data Analysis

Training: Input data is introduced to the network during training, and the network is fine-tuned based on the errors it encounters.

Validation: Detain this phase is employed to assess the network' stability to genera lize and to cease training when generalization ceases to improve.

Testing: Detain the testing phase does not impact the training process, thus of furigana biased evaluation of network performance both during and after training.

## 6. Performance Value for ANN Modelling

Thetablerepresentclassifiedsamplesoffinancialdatasetusedfortrainingtestingandvalidation.

Results

| | Samples | MSE | R |
|---|---|---|---|
| Training: | 5 | 12624.74528e-0 | 9.99659e-1 |
| Validation: | 5 | 18054846.37133e-0 | 9.39282e-1 |
| Testing: | 5 | 2088024.41157e-0 | 9.03881e-1 |

**Table 1:** MSE-MeanSquaredError, R=RegressionCoefficient

(A) (B) (C) (D)

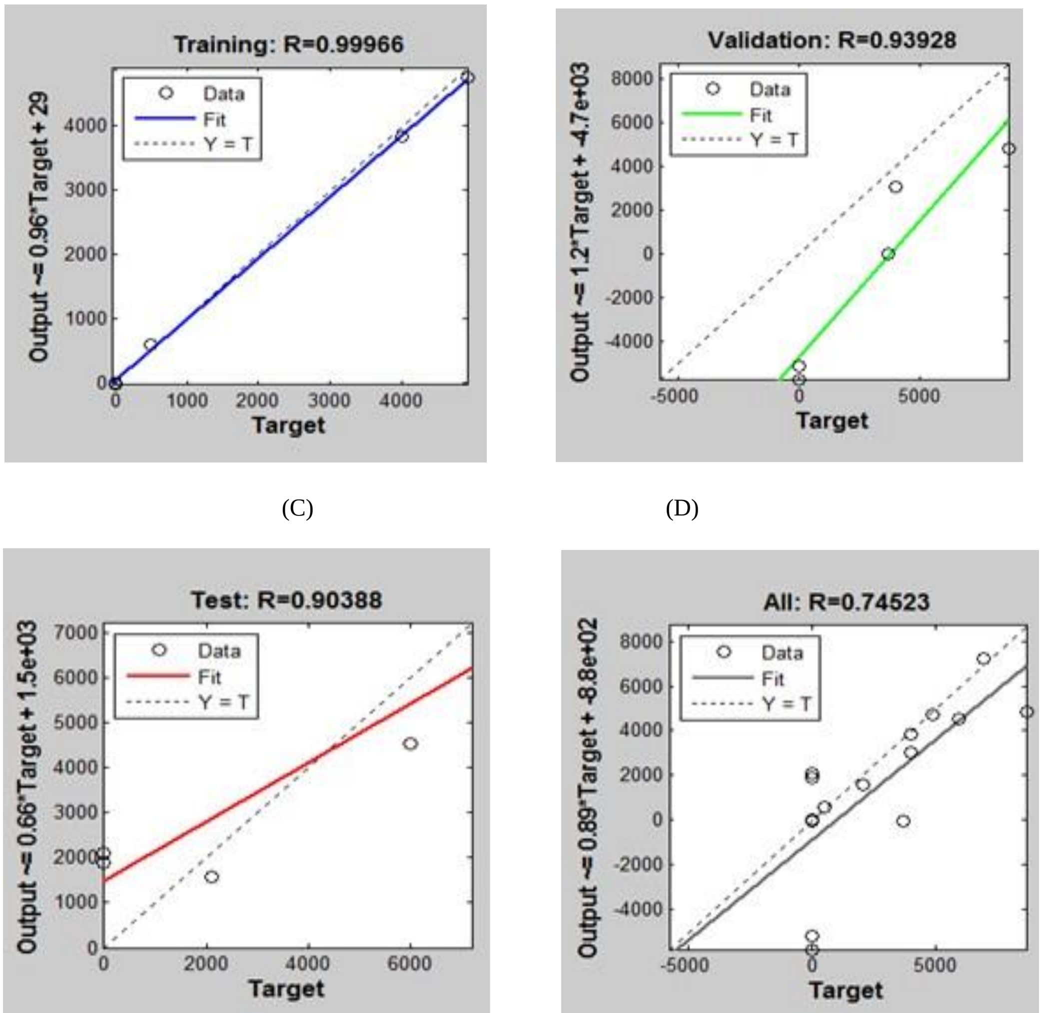


**Fig. 2:** Plot of ANNP redicted Output against Actual Value for (A)Training(B)Validation(C)Testing(D) Target.

ResearchQuestion4:
What are the existing voild or gaps and potential avenues for future research in the domain of Machine Learning-based approaches? Fraud Detection

This section seeks to identify research gaps and outline future directions in the field. The synthesis of reviewed articles reveals limitations and provides insights into potential avenues for future work, as discussed in the following subsections.

Imbalanced Dataset:
Addressing the challenge of imbalanced data, some studies have implemented oversampling approaches [12], while others aim to introduce effective strategies for extremely imbalanced data. For example, Li et al. [86] and Perols [61] utilized imbalanced and left-balancing datasets through the oversampling method for future work. Hence, future studies could explore other oversampling techniques as well as under-sampling methods.

Data Size: Several research works have identified the size of the dataset as a limitation. For instance. The size of a data is a major challenge in many nations. Resolving dataset size issues could lead to improved and more efficient ML approaches for identifying fraudulent financial activities. Many studies in the reviewed literature emphasized that enhancing the performance of detection models can be achieved by improving input vectors. Future work could involve combining data from various sources, such as financial social media sites like Seeking Alpha, numerical information from financial documents, and transcripts of earnings calls, to generate more relevant feature vectors. Unstructured Data: Recent studies have explored different types of unstructured data, such as vocal inputs and textual data. However, unstructured data exploration in financial fraud detection needs more attention for remarkable results. Future research could look into text sources from financial statements and explore the use of new data mining techniques.

Machine-Learning-Based Techniques: Classifying the machine learning techniques used for financial fraud detection is an effective way to determine suitable methods for this research domain. Investigating why certain methods were selected and why others received less attention can identify research gaps. Many learning algorithms that are popular in other fields have not been widely applied in financial fraud detection. Traditional techniques have been used in time past. ANN model is considered one of the best computational intelligence techniques.

For example, active learning, which addresses insufficient data and improves learning cost, incremental learning, which dynamically adds sample data for accuracy, and transfer learning, which uses knowledge from one task to enhance learning in another task, can receive more attention in future research.

4. Discussion: In this section, the systematic literature review's content is highlighted, encompassing popular financial fraud detection techniques and machine learning methods usedin detection. Findings are categorized based on the frequency of usage in ML techniques and types offinancialfraud. The review reveals that, fromyears back the ANN algorithmis the most popular technique for identifying fraudulent activities in the financial sector, followed bySVM.

**Conclusions**

Financial fraud poses significant challenges across various sectors, and its persistence necessitates advanced detection methods. This study systematically reviewed existing literature on machine learning (ML)-based fraud detection, a sample method longwise menstruated using the Artificial neural network. From previous studies, SVM and ANN emerged as popular ML algo rhythms for fraud detection, with credit card fraud being the most common ly studied type. The study identified gaps in research, emphasizing the need for exploration of other algorithms, increased attention to unsupervised learning approaches like clustering, and the utilization of emerging hybrid techniques in future research. ANN analysis was demon started in the study with 70% training, 15 % testing and 15% validation at a reduced error. Inconclusion, ML approaches especially ANN model present promising avenues for enhancing financial fraud detection, contributing to economic stability and societal well-being.

**References**

1. Hilal, W.; Gadsden, S.A.; Yawney, J. Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances. Expert Syst. Appl. 2021, 193, 116429.
2. Ashtiani, M.N.; Raahemi, B. Intelligent Fraud Detection in Financial Statements Using Machine Learning and Data Mining: A Systematic Literature Review. IEEE Access 2021, 10, 72504–72525.
3. Albashrawi, M. Detecting Financial Fraud Using Data Mining Techniques: ADecade Review from 2004 to 2015. J. Data Sci. 2016, 14, 553–570.
4. Choi, D.; Lee, K. An ArtificialIntelligence Approach to Financial Fraud Detection under IoT Environment: A Survey and Implementation. Secur. Commun. Netw. 2018, 2018, 1–15.
5. Ngai, E.W.T.; Hu, Y.; Wong, Y.H.; Chen, Y.; Sun, X. The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decis. Support Syst. 2011, 50, 559–569.
6. Ryman-Tubb, N.F.; Krause, P.; Garn, W. How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark. Eng. Appl. Artif. Intell. 2018, 76, 130–157.
7. M.Okwu., Emovon I. (2018) Artificial Neural Network and Greedy Heuristic Apporach to Transshipment Model in a Bottling Plant. Journal of OperationsResearch and Information Engineering. American Association for Science andTechnology (AASCIT) 1(2) 51-60.
8. Chaquet-ulldemolins, J.; Moral-rubio, S.; Muñoz-romero, S. On the Black-Box Challenge for Fraud Detection Using Machine Learning (II): Nonlinear Analysis through Interpretable Autoencoders. Appl. Sci. 2022, 12, 3856.
9. Da'U, A.; Salim, N. Recommendation system based on deep learning methods: A systematic review and new directions. Artif. Intell. Rev. 2019, 53, 2709–2748.
10. Zeng, Y.; Tang, J. RLC-GNN: An Improved Deep Architecture for Spatial-Based Graph Neural Network with Application to Fraud Detection. Appl. Sci. 2021, 11, 5656.

11. M.O. Okwu, Oreko B.U., Okii, Austin U., Oguoma O. (2019) ANN Model for Cost Optimization in a Dual Source Multi-Destination System., Taylor and Francis Group. 5, 1-13., 1447774.
12. Zhang, D.; Zhou, L. Discovering Golden Nuggets: Data Mining in Financial Application. IEEE Trans. Syst. Man Cybern. Part C Appl. Rev. 2004, 34, 513–522.
13. Olufemi A. (2020) A Comparative Study of Artificial Neural Network (ANN) and Adaptive Neuro-Fuzzy Inference System (ANFIS) Model in Distribution System with Non- Deterministic Inputs, International Journal of Engineering and Business Management, SAGE. Volume 10. 1-17.
14. Ewim D., M. Okwu, Onyiriuka E.J., Abiodun A. (2022). A quick review of the applications of artificial neural networks (ANN) in the modelling of thermal systems, Engineering and Applied Science Research, EASR, 2022;49(3):444-458.
15. Samuel O.D. (2019) Comparison of Response Surface Methodology (RSM) and Artificial Neural Network (ANN) in Modelling of Waste Coconut Oil Ethyl Esthers Production. Taylor and Francis. Energy Sources, Part A: Recovery, Utilization, and Environmental Effects.
16. Popat, R.R.; Chaudhary, J. A Survey on Credit Card Fraud Detection Using Machine Learning. In Proceedings ofthe 2018 2nd InternationalConference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 11–12 May 2018; pp. 1120–1125.
17. 17. Okonkwo C.P., V.Ajiwe, M.Obiadi, M.Okwu, J.Oyogu (2023). Production of biodiesel from the novel using Artificial Neural Network. Journal of Cleaner Production, Elsevier.
18. Gyamfi, N.K.; Abdulai, J. Bank Fraud Detection Using Support Vector Machine. In Proceedings of the 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 1–3 November 2018; pp. 37–41.
19. Carneiro, E.M.; Dias, L.A.V.; Da Cunha, A.M.; Mialaret, L.F.S. Cluster Analysis and Artificial NeuralNetworks: A Case Study in Credit Card Fraud Detection. In Proceedings of the 2015 12th International Conference on Information Technology- New Generations, Mumbai, India, 11–14 December 2011; pp. 122–126.
20. Iyer, D.; Mohanpurkar, A.; Janardhan, S.; Rathod, D.; Sardeshmukh, A. Credit card fraud detection using Hidden Markov Model. In Proceedings of the 2011 World Congress on Information and Communication Technologies, Mumbai, India, 11–14 December 2011; pp. 1062–1066.
21. Patil,S.; Nemade,V.; Soni,P.ScienceDirectPredictiveModellingFor CreditCardFraud Detection Using Data Analytics. Procedia Comput. Sci. 2018, 132, 385–395.
22. Mohammadian, V.; Navimipour, N.J.; Hosseinzadeh, M.; Darwesh, A. Comprehensive and systematic study on the fault tolerance architectures in cloud computing. J. Circuits Syst. Comput. 2020, 29, 2050240.
23. Kitchenham, B.; Charters, S. Guidelines for Performing Systematic Literature Reviews in SoftwareEngineering;Keele University: Keele, UK, 2007;p.65.24.Pourhabibi, T.;Ong, K.-L.; Kam, B.H.; Boo, Y.L. Fraud detection: A systematic literature review of graph-based anomaly detection approaches. Decis. Support Syst. 2020, 133, 113303.
24. Marcotte, P.; Petrillo, F. Multiple Fault-tolerance Mechanisms in Cloud Systems: A Systematic Review. In Proceedings of the 2019 IEEE International Symposium on Software ReliabilityEngineering Workshops (ISSREW), Berlin, Germany, 28–31 October 2019;pp. 414– 421.
25. Isong, B.E.; Bekele, E. A systematic review of fault tolerance in mobile agents. Eng. Appl. 2013, 2, 111–124.
26. Nassif,A.B.;AbuTalib,M.;Nasir,Q.;Dakalbab,F.M.MachineLearningforAnomaly Detection: A Systematic Review. IEEE Access 2021, 9, 78658–78700.
27. Randhawa, K.; Loo, C.K.; Seera, M.; Lim, C.P.; Nandi, A.K. Credit Card Fraud Detection Using AdaBoost and Majority Voting. IEEE Access 2018, 6, 14277–14284.
28. Bhattacharyya, S.;Jha,S.;Tharakunnel, K.;Westland,J.C.Dataminingforcredit cardfraud: A comparative study. Decis. Support Syst. 2011, 50, 602–613.
29. Srivastava, A.; Yadav, M.; Basu, S.; Salunkhe, S.; Shabad, M. Credit card fraud detection at merchant sideusingneuralnetworks. InProceedingsofthe20163rdInternationalConferenceon Computing forSustainableGlobalDevelopment,NewDelhi, India, 16–18March2016;pp. 667– 670.
30. de Sá, A.G.; Pereira, A.C.; Pappa, G.L. A customized classification algorithm for credit card fraud detection. Eng. Appl. Artif. Intell. 2018, 72, 21–29.
31. Robinson, W.N.; Aria, A. Sequential fraud detection for prepaid cards using hidden Markov model divergence. Expert Syst. Appl. 2018, 91, 235–251.
32. Hajek, P.;Henriques, R. Mining corporateannualreportsfor intelligent detectionoffinancial statement fraud—A comparative study of machine learning methods. Knowl.-Based Syst. 2017, 128, 139–152.
33. Craja, P.; Kim, A.; Lessmann, S. Deep learning for detecting financial statement fraud. Decis. Support Syst. 2020, 139, 113421.
34. Ravisankar, P.; Ravi, V.; Rao, G.R.; Bose, I. Detection of financial statement fraud and feature selection using data mining techniques. Decis. Support Syst. 2011, 50, 491–500.
35. Gao, Y.; Sun, C.; Li, R.; Li, Q.; Cui, L.; Gong, B. An Efficient Fraud Identification Method Combining Manifold Learning and Outliers Detection in Mobile Healthcare Services. IEEE Access 2018, 6, 60059–60068.
36. Huang, S.-Y.; Tsaih, R.-H.; Yu, F. Topological pattern discovery and feature extraction for fraudulent financial reporting. Expert Syst. Appl. 2014, 41, 4360–4372.
37. Peng, J.; Li, Q.; Li, H.; Liu, L.; Yan, Z.; Zhang, S. Fraud Detection of Medical Insurance Employing Outlier Analysis. InProceedings ofthe 2018 IEEE 22nd InternationalConference on ComputerSupportedCooperativeWorkinDesign (CSCWD), Nanjing,China,9–11May2018;pp.341–346.

38. van Capelleveen, G.; Poel, M.; Mueller, R.M.; Thornton, D.; van Hillegersberg, J. Outlier detection in healthcare fraud: A case study in the Medicaid dental domain. Int. J. Account. Inf. Syst. 2016, 21, 18–31.
39. Anbarasi, M.S.; Dhivya, S. Fraud detection using outlier predictor in health insurance data.In Proceedings of the 2017 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, India, 23–24 February 2017; pp. 1–6.
40. 41.Sundarkumar, G.G.; Ravi, V.; Siddeshwar, V. One-class support vector machine based undersampling: Application to churn prediction and insurance fraud detection. In Proceedings of the 2015IEEEInternationalConference onComputationalIntelligence and Computing Research (ICCIC), Madurai, India, 10–12 December 2015; pp. 1–7.
41. 42.Subudhi, S.; Panigrahi, S. Effect ofClass Imbalanceness in Detecting Automobile Insurance Fraud. In Proceedings of the 2018 2nd International Conference on Data Science and Business Analytics (ICDSBA), ChangSha, China, 21–23 September 2018; pp. 528–531.
42. Fayyomi, M.; Eleyan, D.; Eleyan, A. A Survey Paper On Credit Card Fraud Detection Techniques. Int. J. Adv. Res. Comput. Eng. Technol. 2021, 3, 827–832.
43. Wang, Y.; Xu, W. Leveraging deep learning with LDA-based text analytics to detect automobile insurance fraud. Decis. Support Syst. 2018, 105, 87–95.
44. Gepp, A.; Kumar, K.; Bhattacharya, S. Lifting the numbers game: Identifying key input variables and a best-performing model to detect financial statement fraud. Account. Financ. 2021, 61, 4601–4638.
45. Perols, L.; Lougee, B.A. The relation between earnings management and financial statement fraud. Adv. Account. 2011, 27, 39–53.
46. Wang, Q.; Xu, W.; Huang, X.; Yang, K. Enhancing intraday stock price manipulation detection by leveraging recurrent neural networks with ensemble learning. Neurocomputing 2019, 347, 46–58.
47. Islam, S.R.; Ghafoor, S.K.; Eberle, W. Mining Illegal Insider Trading ofStocks: AProactive Approach. In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 10–13 December 2018; pp. 1397–1406.
48. Kulkarni, P.M.; Domeniconi, C. Network-based anomaly detection for insider trading. arXiv 2017, arXiv:1702.05809.
49. Mirtaheri, M.; Abu-El-Haija, S.; Morstatter, F.; Steeg, G.V.; Galstyan, A. Identifying and Analyzing Cryptocurrency Manipulations in Social Media. IEEE Trans. Comput. Soc. Syst. 2021, 8, 607–617.
50. Monamo, P.M.; Marivate, V.; Twala, B. A Multifaceted Approach to Bitcoin Fraud Detection: Global and Local Outliers. In Proceedings of the 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA), Anaheim, CA, USA, 18–20 December 2016; pp. 188–194.
51. Vasek, M.; Moore, T. There’s No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams BT–Financial Cryptography and Data Security. In Proceedings of the International Conference on Financial Cryptography and Data Security, Kota Kinabalu, Malaysia, 1–5 March 2015; pp. 44–61.
52. Monamo, P.; Marivate, V.; Twala, B. Unsupervised learning for robust Bitcoin fraud detection. In Proceedings of the 2016 Information Security for South Africa (ISSA), Johannesburg, South Africa, 17–18 August 2016; pp. 129–134.
53. Li, X.;Ying, S. Lib-SVMs DetectionModelofRegulating-Profits FinancialStatement Fraud Using Data of Chinese Listed Companies. In Proceedings of the 2010 International Conference on E-Product E-Service and E-Entertainment, Henan, China, 7–9 November 2010; pp. 1–4.
54. Throckmorton, C.S.; Mayew, W.J.; Venkatachalam, M.; Collins, L.M. Financial fraud detection using vocal, linguistic and fi nancial cues. Decis. Support Syst. 2015, 74, 78–87.
55. Glancy, F.H.; Yadav, S.B. A computational model for fi nancial reporting fraud detection. Decis. Support Syst. 2011, 50, 595–601.
56. Mareeswari, V.; Gunasekaran, G. Prevention ofcredit card fraud detection based on HSVM. In Proceedings of the 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, India, 25–26 February 2016; pp. 1–4.
57. Humpherys, S.L.; Mof, K.C.; Burns, M.B.; Burgoon, J.K.; Felix, W.F. Identi fi cation of fraudulent fi nancial statements using linguistic credibility analysis. Decis. Support Syst. 2011, 50, 585–594.
58. Li, X.;Xu, W.;Tian, X. Howto protect investors?AGA-based DWD approach for financial statement fraud detection. In Proceedings of the 2014 IEEE International Conference onSystems, Man, and Cybernetics (SMC), San Diego, CA, USA, 5–8 October 2014; pp. 3548– 3554.
59. Karlos, S.;Fazakis, N.;Kotsiantis, S.;Sgarbas, K. Semi-supervised forecasting of fraudulent financial statements. In Proceedings ofthe 20th Pan-Hellenic Conference onInformatics, Patras, Greece, 10–12 November 2016.
60. Özçelik, M.H.; Duman, E.; I¸sik, M.; Çevik, T. Improving a credit card fraud detection system using genetic algorithm. In Proceedings of the 2010 International Conference on Networking and Information Technology, Manila, Philippines, 11–12 June 2010; pp. 436–440.
61. Rizki, A.; Surjandari, I.; Wayasti, R.A. Data mining application to detect financial fraud in Indonesia’s public companies. In Proceedings of the 2017 3rd International Conference on Science in Information Technology (ICSITech), Bandung, Indonesia, 25–26 October 2017; pp. 206–211.
62. Chen, S. Detectionoffraudulent financial statementsusing the hybrid data mining approach. SpringerPlus 2016, 5, 1–16.
63. Yao, J.; Zhang, J.; Wang, L. A financial statement fraud detection model based on hybrid data mining methods. In Proceedings of the 2018 international conference on artificial intelligence and big data (ICAIBD), Chengdu, China, 26–28 May 2018; pp. 57–61.
64. Rajak, I.; Mathai, K.J. Intelligent fraudulent detection

system based SVM and optimized by danger theory. In Proceedings of the 2015 International Conference on Computer, Communication and Control (IC4), Indore, India, 10–12 September 2015; pp. 1–4.
65. Jeragh, M.; Alsulaimi, M. Combining Auto Encoders and One Class Support Vectors Machine for Fraudulant Credit Card Transactions Detection. In Proceedings ofthe 2018 Second World Conference on Smart Trends in Systems, Securityand Sustainability(WorldS4), London, UK, 30–31 October 2018; pp. 178–184.
66. Kho, J.R.D.; Vea, L.A. Credit card fraud detection based on transaction behavior. In Proceedings of the TENCON 2017-2017 IEEE Region 10 Conference, Penang, Malaysia, 5–8 November 2017; pp. 1880–1884.
67. Behera, T.K.; Panigrahi, S. Credit Card Fraud Detection: A Hybrid Approach Using Fuzzy Clustering & Neural Network. In Proceedings of the 2015 Second International Conference on Advances in Computing and Communication Engineering, Dehradun, India, 1–2 May 2015; pp. 494–499.
68. HaratiNik, M.R.; Akrami, M.; Khadivi, S.; Shajari, M. FUZZGY: A hybrid model for credit card fraud detection. InProceedings ofthe 6thInternationalSymposiumonTelecommunications (IST), Tehran, Iran, 6–8 November 2012; pp. 1088–1093.
69. Malini, N.;Pushpa, M. Analysisoncredit cardfraudidentificationtechniquesbasedonKNN and outlier detection. In Proceedings of the 2017 third international conference on advances in electrical, electronics, information, communication and bio-informatics (AEEICB), Chennai, India, 27–28 February 2017; pp. 255–258.
70. Benchaji, I.; Douzi, S.; ElOuahidi, B. Using Genetic Algorithm to Improve Classification of Imbalanced Datasets for Credit Card Fraud Detection. In Proceedings of the International Conference on Advanced Information Technology, Services and Systems, Mohammedia, Morocco, 17–18 October 2018; pp. 1–5.
71. Case, B.RecognizingDebit CardFraudTransactionUsingCHAIDand K-Nearest Neighbor: Indonesian Bank case. In Proceedings of the 2016 11th InternationalConference on Knowledge, Information and Creativity Support Systems (KICSS), Yogyakarta, Indonesia, 10–12 November 2016.
72. Bhusari, V.; Patil, S. Study of Hidden Markov Model in credit card fraudulent detection. In Proceedings of the 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), Coimbatore, India, 29 February–1 March 2016; pp. 1–4.
73. Sahin, Y.;Bulkan, S.;Duman, E. Acost-sensitive decisiontree approachfor fraud detection. Expert Syst. Appl. 2013, 40, 5916–5923.
74. Duman, E.; Ozcelik, M.H. Detecting credit card fraud by genetic algorithm and scatter search. Expert Syst. Appl. 2011, 38, 13057–13063.
75. Sahin, Y.; Duman, E. Detecting credit card fraud by ANN and logistic regression. In Proceedings of the 2011 International Symposium on Innovations in Intelligent Systems and Applications, Istanbul, Turkey, 15–18 June 2011; pp. 315–319.
76. Ghobadi, F.; Rohani, M. Cost sensitive modeling of credit card fraud using neural network strategy. In Proceedings of the 2016 2nd International Conference of Signal Processing and Intelligent Systems (ICSPIS), Tehran, Iran, 14–15 December 2016; pp. 1–5.
77. Awoyemi, J.O.; Adetunmbi, A.O.; Oluwadare, S.A. Credit card fraud detection using machine learning techniques: A comparative analysis. In Proceedings of the 2017 international conference on computing networking and informatics (ICCNI), Ota, Nigeria, 29–31 October 2017; pp. 1–9.
78. Mishra, A.; Ghorpade, C. Credit Card Fraud Detection on the Skewed Data Using Various ClassificationandEnsembleTechniques.InProceedingsofthe2018IEEEInternational
79. Students'ConferenceonElectrical, ElectronicsandComputerScience(SCEECS),Bhopal, India, 24–25 February 2018; pp. 1–5.
80. Kirlidog, M.; Asuk, C. A Fraud Detection Approach with Data Mining in Health Insurance. Procedia-Soc. Behav. Sci. 2012, 62, 989–994.
81. Peng, H.; You, M. The Health Care Fraud Detection Using the Pharmacopoeia Spectrum Tree and Neural Network Analytic Contribution Hierarchy Process. In Proceedings of the 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, China, 23–26 August 2016; pp. 2006–2011.
82. Bauder, R.; da Rosa, R.; Khoshgoftaar, T. Identifying Medicare Provider Fraud with Unsupervised Machine Learning. In Proceedings of the 2018 IEEE International Conference on InformationReuse and Integration(IRI), Salt Lake City, UT, USA, 7–9 July 2018;pp. 285–292.
83. Bauder, R.A.; Khoshgoftaar, T.M.; Richter, A.; Herland, M. Predicting Medical Provider Specialties to Detect Anomalous Insurance Claims. In Proceedings of the 2016 IEEE 28th InternationalConference on Tools with ArtificialIntelligence (ICTAI), San Jose, CA, USA, 6–8 November 2016; pp. 784–790.
84. Badriyah, T.; Rahmaniah, L.; Syarif, I. Nearest Neighbour and Statistics Method based for Detecting Fraud in Auto Insurance. In Proceedings of the 2018 International Conference on Applied Engineering (ICAE), Batam, Indonesia, 3–4 October 2018; pp. 1–5.
85. Zhou, Y.; Wang, X.; Zhang, J.; Zhang, P.; Liu, L.; Jin, H.; Jin, H. Analyzing and Detecting Money-Laundering Accounts in Online Social Networks. IEEE Netw. 2017, 32, 115–121.
86. Mhamane, S.S.; Lobo, L.M.R.J. Internet banking fraud detection using HMM. In Proceedings of the 2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12), Karur, India, 26–28 July 2012; pp. 1–4.
87. Faraji, Z.; States, U. A Review of Machine Learning Applications for Credit Card Fraud Detection with A Case study. J. Manag. 2022, 5, 49–59.