Original Article

Data Mining-based Financial Statement Fraud Detection: Systematic Literature Review and Meta-analysis to Estimate Data Sample Mapping of Fraudulent Companies Against Non-fraudulent Companies

Global Business Review
1–24
© 2021 IMI
Reprints and permissions:
in.sagepub.com/journals-permissions-india
DOI: 10.1177/0972150920984857
journals.sagepub.com/home/gbr
SAGE

Sonika Gupta[1] and Sushil Kumar Mehta[2]

Abstract

Data mining techniques have proven quite effective not only in detecting financial statement frauds but also in discovering other financial crimes, such as credit card frauds, loan and security frauds, corporate frauds, bank and insurance frauds, etc. Classification of data mining techniques, in recent years, has been accepted as one of the most credible methodologies for the detection of symptoms of financial statement frauds through scanning the published financial statements of companies. The retrieved literature that has used data mining classification techniques can be broadly categorized on the basis of the type of technique applied, as statistical techniques and machine learning techniques. The biggest challenge in executing the classification process using data mining techniques lies in collecting the data sample of fraudulent companies and mapping the sample of fraudulent companies against non-fraudulent companies. In this article, a systematic literature review (SLR) of studies from the area of financial statement fraud detection has been conducted. The review has considered research articles published between 1995 and 2020. Further, a meta-analysis has been performed to establish the effect of data sample mapping of fraudulent companies against non-fraudulent companies on the classification methods through comparing the overall classification accuracy reported in the literature. The retrieved literature indicates that a fraudulent sample can either be equally paired with non-fraudulent sample (1:1 data mapping) or be unequally mapped using 1:many ratio to increase the sample size proportionally. Based on the meta-analysis of the research articles, it can be concluded that machine learning approaches, in comparison to statistical approaches, can achieve better classification accuracy, particularly when the availability of sample data is low. High classification accuracy can be obtained with even a 1:1 mapping data set using machine learning classification approaches.

[1] School of Computer Science and Engineering, Shri Mata Vaishno Devi University, Katra, Jammu and Kashmir, India.
[2] School of Business, Shri Mata Vaishno Devi University, Katra, Jammu and Kashmir, India.

Corresponding author:
Sonika Gupta, School of Computer Science and Engineering, Shri Mata Vaishno Devi University, Katra, Jammu and Kashmir 182320, India.
E-mail: sonika.gupta@smvdu.ac.in

Keywords

Classification accuracy, data mining, data sample mapping scheme, financial statement frauds, machine learning approaches, statistical approaches

Introduction

Financial frauds, also known as 'business frauds', can be categorized as financial statement manipulations, cash embezzlement, assets manipulation or alternation. Generally, it has been observed that the internal members of an organization manipulate the financial records with the intention of committing fraud (Spathis, 2002). The motivation to commit a financial fraud varies from inflating the income and profits to reducing tax payments or inflating the stock price and credit ratings (Agrawal & Chatterjee, 2015). Financial frauds may also be committed with a motivation of personal gain by the internal management (Das et al., 2018).

Financial frauds are not novel frauds, and such frauds have been in existence since the time of evolution of business (Rezaee & Riley, 2009). The broad categories of financial frauds are presented in Figure 1.

Frauds deliberately committed by any person or an institution with the motive of secretly deceiving a bank or any such financial institution is defined as 'bank fraud' by Phua et al. (2010). Phua et al. (2010) have also stated that corporate frauds include intentionally misrepresenting the financial information of a company in order to deceive the public, in general, or the stakeholders of the company such as investors, shareholders, et cetera, with a basic motive of increasing the monetary gains of the company at large or at a personal level. The research work of Ngai et al. (2011) is based on insurance frauds, and states that an insurance fraud is committed by an insured to gain undue advantages from the insurer through raising a fraudulent claim, or the insurer can also commit this fraud knowingly through denying the due benefits to the insured.

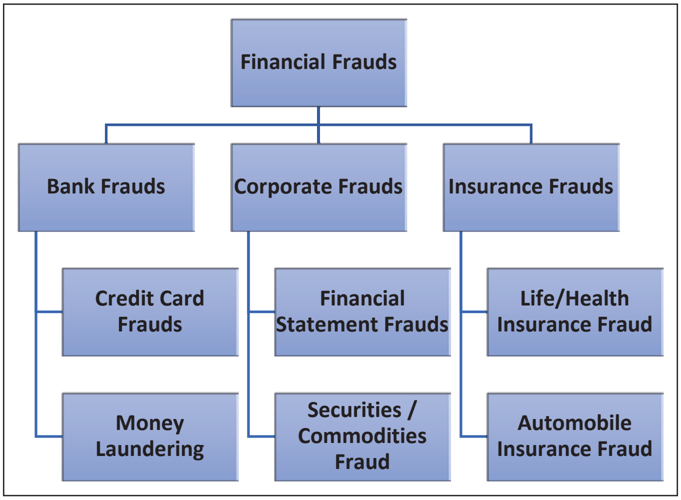
Financial Frauds
Bank Frauds
Corporate Frauds
Insurance Frauds
Credit Card Frauds
Money Laundering
Financial Statement Frauds
Securities / Commodities Fraud
Life/Health Insurance Fraud
Automobile Insurance Fraud

Figure 1. Categories of Financial Frauds.

Source: Federal Bureau of Investigation (2010–2011), Financial Crimes Report (2010–2011), USA.

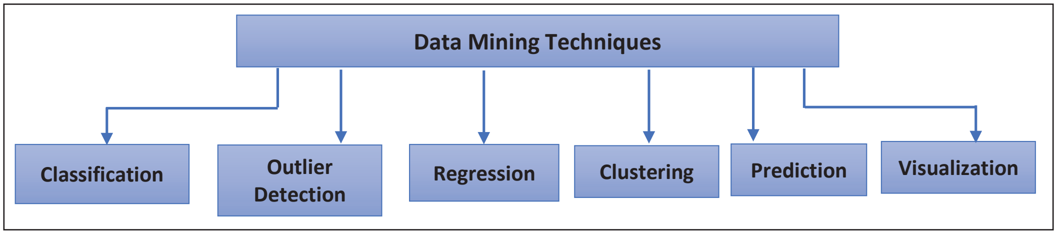

Figure 2. Categorization of Data Mining Techniques Used to Discover Financial Frauds.

Source: The author.

The literature survey (Zhang & Zhou, 2004; Yamanishi et al., 2004; Yue et al., 2007; Han et al., 2011) shows that the major emphasis in the process of detection of financial statement frauds has been on utilizing data mining techniques, which have proven quite effective not only in detecting financial statement frauds but also in discovering other financial crimes which may involve frauds pertaining to fake or bounced cheques, credit card frauds, loan and securities frauds, corporate frauds, bank and insurance frauds, et cetera. Zhou and Kapoor (2011) have emphasized that it is feasible to detect unknown underlying patterns from the data and predict future trends and behaviours through using data mining tools and techniques.

Different types of data mining techniques can be used to discover financial frauds. Based on the survey of the literature, the data mining techniques are categorized as indicated in Figure 2.

Zhang and Zhou (2004) and Kumar and Verma (2012) defined classification as a mechanism of evaluating and finding out common characteristics that clearly differentiate various sets of data classes. Using classification, it is thus feasible to create a model that can be used to classify unknown data sets into specific categories or classes (Kumar & Verma, 2012; Rahman & Afroz, 2013). These categorical labels are distinct and not in any specific order, and nor are they defined a priori. The most widely used techniques for classification include regression, support vector machines (SVM), artificial neural networks (ANN), decision trees and the Naive Bayes technique (Han et al., 2011; Rahman & Afroz, 2013).

The K-nearest-neighbour, Naive Bayes and self-organizing map techniques use clustering analysis, which primarily deals with the issue of devising strategy to divide a multivariate data set into groups such that data elements within a group are quite similar, whereas there is a significant amount of dissimilarity with the data elements divided in other groups according to Yue et al. (2007). The clustering technique is used to split data into separate groups (clusters) which have significant disparity between them, while the related data are clustered within a group (Biswas et al., 2020). At times, clustering is considered a variant of unsupervised classification.

A data element whose characteristics are entirely dissimilar from or inconsistent with the rest of the elements present in the data set, including the neural networks and logistic forecasting models (Kotsiantis et al., 2006), is called an outlier. Outlier detection is a methodology to identify data elements that are distinct from the group under observation. Yamanishi et al. (2004) concluded that the issue of detecting an outlier/anomaly is critical in the field of data mining.

Gray and Debreceny (2014) provided a taxonomy to identify the different types of financial fraud schemes which can be mined from the various evidential records of a company and provided a comprehensive guideline on areas where the data mining technique can be applied effectively to detect frauds. According to Gray and Debreceny (2014), data mining tools can be very effective in resolving financial frauds committed through manipulation of the journal entries, especially the ones that are recorded in multiple accounts or those involving reversing of entries. Classification of data mining techniques, in recent years, has been accepted as one of the most credible methodologies for the detection of financial statement frauds (Ngai et al., 2011; Phua et al., 2010; Phyu, 2009; Zhou & Kapoor, 2011).

The purpose of this study is to provide a systematic literature review (SLR) of the articles published (since 1995) related to financial statement fraud detection using data mining techniques and apply the SLR technique as proposed by Kitchenham et al. (2009). The reviewed articles were studied particularly from the perspective of classification of fraudulent companies using financial data/ratios. The authors have also surveyed a few studies, with high citations, that have used textual data from financial reports.

Further, a meta-analysis has been performed to estimate the data sample mapping ratio of fraudulent companies against non-fraudulent companies. With the objective of estimating the data sample mapping ratio, three features were noted from each reviewed article, namely the data mining technique applied, the size of the data sample, along with the data sampling ratio used in the literature, and the overall classification accuracy in terms of accuracy percentage achieved in the study.

The subsequent sections of the article are as follows. The second section indicates the objectives, while in the third section, the methodology of SLR is described. The fourth section presents the SLR of the studies related to detection of financial statement frauds. The fifth section describes the meta-analysis of the literature survey. A discussion of the meta-analysis is provided in the sixth section. The seventh section includes the final conclusions, followed by managerial implications in the eighth section and limitations and future research directions in the ninth section.

Objectives

The main objective of this review is to primarily identify the techniques of classifications that have been applied widely in the field of financial statement fraud detection. Further, through this survey, the authors desire to establish the relationship between data sample mapping of fraudulent companies and that of non-fraudulent companies and its impact on the overall accuracy of data analysis using machine learning approaches vis-à-vis statistical approaches.

Methodology

In this study, the SLR has been performed following the guidelines applied in Kitchenham et al. (2009). For performing the SLR, the following steps were undertaken:

> **Step 1: Framing of research question**—One of the most critical aspects of the SLR process is the framing of the correct set of questions which would actually set the direction and focus of the survey. The focus of the authors' questions was mainly to establish the types of financial frauds and the different types of data mining techniques and approaches that have been used to detect financial frauds, along with their relative effectiveness. One of the focus points of the questions was to establish the data mining approach that results in better classification accuracy, specifically in cases where the availability of sample data is low.
>
> **Step 2: Selection of research articles**—The relevant research articles published in various conference proceedings and journals of repute were included in this study. The main criteria of selection were to select articles that were relevant and/or considerably cited across academia. This search process was conducted manually.

Step 3: Detailed review of literature to collect relevant data to perform meta-analysis—The data on the technique/model applied, the size of the data sample and the mapping ratio used, along with overall classification accuracy achieved using the technique/model, were extracted from each study under consideration. The detailed review of literature (from 1995 onwards) is presented in the fourth section.

Step 4: Data analysis—For the purpose of performing the meta-analysis, the data were tabulated to present the name of the researcher along with the year of research, the data mining algorithm/method applied for classification, the details of the overall data sample size and the total number of fraudulent and non-fraudulent companies, with the mapping ratio as 1:1, if the total number of fraudulent companies matched the total number of non-fraudulent ones, and as 1:many, if the total number of fraudulent companies was not the same as the total number of non-fraudulent companies, and lastly the classification accuracy as reported in the literature. Further, the analysis was performed after presenting the data graphically to address the research questions framed in step 1.

Review of Literature

Persons (1995) used the method of logistic regression to detect fraudulent companies. One hundred and three fraudulent firms were identified, which were then equally matched with non-fraudulent firms, and the comparison was done based on the industry group and time span. Ten variables, including eight financial ratios, were experimented with and utilized to generate two logistic regression–based models, one of which was for the year when the fraud occurred and the other for the year prior to the year of fraud. The performance of the mechanism was reasonable, with 64% of the fraudulent companies being classified correctly, while the overall performance was rated at 71.5%.

Green and Choi (1997) created a model for classification of fraudulent firms which had its foundation in the technique of utilizing ANN and endogenous financial data. They acquired the information regarding the financial statements of those firms that had filed with SEC (Securities and Exchange Commission) and at a later stage had been found to contain fraudulent account balances. The study utilized five ratios as input, along with three accounts as input variables. Forty-six fraudulent companies were sampled, along with 49 non-fraudulent companies, and a fraudulent company classification accuracy of 68.4% was observed, with a 71.7% overall accuracy of the model. The researchers concluded that ANN has the potential to be utilized as a tool for detecting fraudulent firms.

Summers and Sweeney (1998) identified a total of 51 companies, based on *The Wall Street Journal*, which were then matched with a control sample for hypothesis testing which was based on a cascaded logistic regression–based model with the objective of ascertaining if any relationship could be observed between allegations of insider trading and financial frauds. The control sample was drawn from the pool of companies on the CompuStat data files. The researchers utilized Altman Z-scores and created three separate logit models. They were able to conclude that in the case of firms that were found to be fraudulent, the instances of insiders selling their stocks of the firm to reduce their exposure to the financial fraud were high. A classification accuracy of 67.8% was observed, and the overall accuracy of the model was low at 59.8%.

Beneish (1999) used the methodology of probit regression for a sample of 2,406 firms, out of which 74 fraudulent firms were identified, whereas the other 2,332 were non-fraudulent. Using probit regression, a classification accuracy of 54.2% and an overall accuracy of 89.5% were attained. Further, the researcher concluded that overstatement leads to inflated prices and that in firms overstating earnings, generally the managers sell their shares just prior to the discovery of fraud.

Spathis (2002) applied the methodology of logistic regression to develop a model for identifying the factors related to financial frauds. Data for the study were obtained from the e-reports filed by the auditors; thus, accessibility of information was high. The sample consisted of 38 fraudulent firms and the same number of non-fraudulent firms, and a total of 10 financial variables were selected. A classification accuracy of 64.3% was observed, and an overall model accuracy of 75.4% was reported. Spathis (2002) also reported that the availability of the ratio of inventory to sales was a useful ratio, as any change in this ratio enabled the auditor to get an idea about the accuracy of the inventory. The researcher also recommended the usage of other techniques for financial fraud detection, including discriminant analysis, adaptive logit networks, neural networks and multi-criteria analysis (Bolton & Hand, 2002; Coderre, 1999).

Lin et al. (2003) used fuzzy neural networks to build a model for the classification of fraudulent and non-fraudulent firms and did a comparative study by using the logistic regression methodology too. The sample included 40 fraudulent and 160 non-fraudulent companies. The comparative analysis indicated that the classification accuracy for non-fraudulent firms using the fuzzy neural network technique was as high as 86.3%, but the classification accuracy for fraudulent companies was low at 35%. In the case of the logistic regression technique, these figures were 97.5% and a very poor 5%, respectively. The analysis was further enhanced with various ratios of fraudulent to non-fraudulent companies, varying from 1:1 to 1:100. The study concluded that the cost of implementation of the logistic regression model and the fuzzy neural network model increased significantly with an enhancement in the ratio of the sample size of fraudulent companies to that of non-fraudulent companies, the cost being slightly less in the case of logistic regression.

Kaminski et al. (2004) used the technique of discriminant analysis to build a model for the classification of firms that may have committed financial fraud; however, the focus of the study was more on investigating the right set of ratios for the purpose of classification. The sample included 40 fraudulent and 160 non-fraudulent companies. As the number of ratios chosen initially was large (21 ratios), the need for multivariate analysis was correctly identified, and discriminant analysis was chosen as the methodology for testing the hypothesis put forth by the researchers regarding the variables. There were significant limitations to the study that offered the conclusion that utilizing ratios may not be a very good mechanism for detecting financial fraud. The model proposed by the researchers did not produce good results, and the classification error was quite high.

Kirkos et al. (2007) undertook a study to explore and perform a comparative analysis between the performances of three popular data mining techniques, namely decision trees, neural networks and Bayesian belief networks, for the purpose of detection of manipulated financial statements while utilizing the financial data published in the public domain. The sample consisted of 76 companies: 38 fraudulent and 38 non-fraudulent. The results indicated that the classification accuracy of the model using Bayesian belief networks was as high as 90.3% of the validation sample, whereas the classification accuracy of the model using neural networks was about 80%, and in the case of the decision tree model the classification accuracy was 73.6%. This led to the conclusion that with a comparatively small number of selected financial ratios, it is feasible to improve the success rate of the classification results. Thus, with an appropriate choice of the financial ratios, coupled with specific data mining techniques, it is possible to develop models that have the capability of achieving a high degree of accuracy in the classification process.

Ata and Seyrek (2009) conducted a study in the Turkish context using a sample of 100 Turkish companies, including 50% fraudulent ones, in the manufacturing sector and listed on the Istanbul Stock Exchange, with the objective of utilizing computer-based data mining techniques for detection of fraudulent financial statements. The decision tree and neural networks methodologies were utilized. The study concluded that the leverage ratio and the return-on-assets ratio are the fundamental ratios in revealing financial statement fraud.

Gaganis (2009) utilized Bayesian networks–based and SVM-based classification models. The study also utilized discriminant analysis, logistic regression, the nearest-neighbour framework, the neural networks framework and univariate and multivariate statistical tools. A total of 199 fraudulent Greek companies were paired randomly through matching the year, sector and approximate size of the companies with those of the non-fraudulent companies. The data set was divided into a training set consisting 234 companies, and the results of the model were validated using the data for the rest of the companies. Seven financial ratios and six non-financial variables in combination with 10 classification algorithms were utilized. The classification accuracy of each algorithm was computed under two scenarios. First, by excluding the non-financial variables, the classification accuracy for fraudulent firms was observed within the range of 76.83%–87.20%. The researcher demonstrated the importance of non-financial variables through building a model with financial ratios and non-financial variables which enhanced the classification accuracy, and results with accuracy ranging between 84.15% and 90.24% were achieved. UTilités Additives DIScriminantes (UTADIS) and probabilistic neural networks (PNN) were found to achieve the highest overall accuracy at 90.24%.

Cecchini et al. (2010) developed a model based on SVM with a specially designed kernel meant for detecting financial statement frauds. This was done through collecting a large amount of empirical data of fraudulent and non-fraudulent companies from the public domain. This data set was used to form the learning data set for machine learning while tweaking the kernel such that the mapping of non-linear points to higher-dimensional features' space was implicitly allowed. The classification accuracy of fraudulent cases was 80%, while that of non-fraudulent cases was 90.6%, thus proving their assertion that with SVM and a custom-designed kernel, a high classification accuracy with publicly available quantitative financial attributes was feasible. The researchers also convincingly demonstrated the ability of the scheme to generate predictive value based on historical data.

Dikmen and Küçükkocaoğlu (2010) conducted a study in the Turkish context with a sample of 126 Turkish manufacturing companies in the period 1992–2002 after obtaining a list of fraudulent companies identified by the Istanbul Stock Exchange. The objective of the study was to develop a model for detecting financial fraud, for which the three-phase cutting plane algorithm was proposed. The study was able to project significant ratios to be used for the model based on the feature selection algorithm and was able to show that the performance of the three-phase cutting plane algorithm was better than that of the existing statistical techniques.

Ravisankar et al. (2011) presented a detailed comparative analysis of various techniques, including SVM, PNN, genetic programming, logistic regression, et cetera, to detect and predict financial statement fraud in firms, for which they utilized the data of 202 Chinese companies with 101 fraudulent companies. The t-statistic technique was utilized for feature subset selection. For the purpose of validation, 10-fold cross-validation was performed at every stage. The study was able to demonstrate that the usage of PNN gave much better and more accurate classification and predicative results, with the accuracy going as high as 98.09%, while genetic programming was also fairly effective with the accuracy of prediction as high as 94.14%. The study suggested that the use of text mining along with data mining could actually prove to be much more accurate, besides resulting in a situation where early warning could be provided regarding a possible situation of financial fraud.

Dechow et al. (2011) used the methodology of logistic regression to calculate the probability of financial manipulation, which was turned into F-scores through utilizing the probabilities of financial fraud in such circumstances, obtained in prior. The researches started out with a large set of variables, which they pruned eventually to a much smaller subset of explanatory variables in a step-by-step manner through discarding at each step the variables that were statistically insignificant. The sample data consisted of 79,651 firms, of which 293 were fraudulent and 79,358 were non-fraudulent. The classification accuracy observed with this technique was 73.8%. The researchers also hypothesized that the change in inventory must not be ignored, as it is indirectly linked to the earnings, which, as the literature survey indicates, is the most commonly manipulated parameter in the case of financial frauds.

Perols (2011) analysed the performance of six statistical and machine learning approaches for detection of financial frauds by initially including 42 different ratio variables. Out of the 42 ratios, only six ratios proved to be significant in classifying the data. The data were tested in the study through computing the misclassification cost. The results of the research proved that logistic regression and SVM outperformed the other approaches, especially ANN, in classifying the fraudulent and non-fraudulent companies correctly.

Zhou and Kapoor (2011) proposed a multi-stage adaptive framework to be employed for fraud detection. The framework is based on response surface methodology, which consists of experimental strategies for analysing independent variables, empirical statistical modelling and optimization methods for finding values of process variables. The authors also proposed a future line of advancement based on an active discovery module, which would detect potential future fraudsters without complete reliance on historical data.

Gupta and Gill (2012) conducted a study in the US context to develop a methodology to detect financial statement fraud. For the study, the researchers chose the financial data of 114 organizations from which they selected a total of 62 features. Using the analysis of variance (ANOVA) mechanism, they were able to reduce the significant number of features to 35 and concluded that these variables were sufficient for determining the status of a firm in case it had committed a financial statement fraud. The researchers further used three techniques of data mining, namely decision tree, Naive Bayes classifier and genetic programming, for detection of fraud and recommended the usage of decision tree for feature extraction.

Mohammed and Kim-Soon (2012) conducted a study in the Malaysian context, using a sample of 44 firms listed on the Malaysia Stock Exchange and secondary data obtained from the financial reports available in the Malaysian Stock Exchange library. The choice of the firms was based on stratified random sampling. The researchers used the Edward Altman model (Altman et al., 1998) for performing the analysis, while also using the paired t-test to analyse if there was parity between the results of Altman's model and current liquidity ratio for assessing the financial status of the firms.

Mehta et al. (2012) conducted a study of financial statement fraud in the Indian context wherein the researchers used the technique of multivariate logistic regression to create a model for detecting fraud. The researchers chose for their sample 60 companies listed on the Bombay Stock Exchange (BSE), 30 fraudulent and 30 non-fraudulent, and obtained the financial-statement data from the audited statements submitted by these firms to the BSE. A total of 10 variables were identified during the study to develop the logistic regression–based model, and these variables were chosen by the researchers primarily based on the previous studies conducted by Spathis (2002) and Ravisankar et al. (2011). The classification accuracy for fraudulent firms was reported as 64%, while the overall accuracy was reported as 71.5%. Considering that this was virtually the first reasonable study conducted in the Indian context, the results were studied carefully. The researchers concluded upon the likelihood of firms with certain characteristics to be more susceptible to indulging in financial statement fraud.

Dalnial et al. (2014) conducted a study in the Malaysian context to understand the process of financial fraud detection. The sample consisted of public listed firms on Bursa Malaysia, the Malaysian stock exchange. Financial data of the listed firms between the years 2000 and 2011 were utilized, and the researchers used multiple linear regression. They were able to show that leverage proxies by total debt to total equity was a significant indicator for fraud analysis, which was found to be consistent with the results obtained by Spathis (2002), and similarly, their conclusion that firms with higher debt-to-equity ratios were more susceptible towards financial statement manipulation was in line with Fanning and Cogger (1998). The overall classification accuracy was found to be 74.7%, while the classification accuracy was 85.7% for fraudulent companies and 51.3% for non-fraudulent firms. The researchers listed a few more variables that they found to be useful for fraud detection. They also expressed their misgivings that there were certain limitations to the study based on the fact that the sample size was small, as sufficient data were not available. Further, the study was based on the fraudulent firms already identified by Bursa Malaysia, indicating that other financial frauds may have been missed.

Nia (2015) conducted a study on financial statement fraud based on the financial statements of firms listed on the Tehran stock exchange. The sample data were taken off the financial statements of 134 firms for the period 2009–2014. The researcher explored the significant differences between the mean of financial ratios of fraudulent and non-fraudulent companies and used the independent sample t-test to test the hypothesis. The study concluded that certain ratios, such as those of current assets to total assets, inventory to total assets, revenue to total assets, total debt to total assets and total debt to total equity, were significant in differentiating between the statements of fraudulent and non-fraudulent firms, whereas some other ratios, such as those of net profit to revenue, total debt to total equity, total debt to total assets, receivables to revenue and working capital to total assets, were insignificant. The researcher also concluded that in certain cases, the study findings did not match with the findings of previous studies and alluded the same to the weakness of the corporate governance structure in Iranian firms.

Kanapickienė and Grundienė (2015) conducted their study on 165 firms in Lithuania, out of which 40 were fraudulent and 125 were non-fraudulent, with the objective of identifying the financial ratios that could enable detection of financial statement frauds, through utilizing the method of logistic regression. The period under investigation for these firms was 1998–2009. A total of 51 financial ratios were explored, and the 32 significant ratios which could enable detection of financial statement fraud were identified with reference to the Lithuanian firms. The overall classification accuracy was observed to be 64%, while the classification accuracy for fraudulent firms was observed to be 69%.

Lin et al. (2015) used the tools like questionnaires and data mining to extract the contextual and financial features of frauds and then ranked the features based on their importance through using logistic regression, classification and regression tree (CART) and ANN for fraud detection. The data sample was taken from Taiwan Securities for the period 1998–2010 and included a total of 576 companies, out of which 129 were fraudulent, keeping the ratio of fraudulent cases to non-fraudulent cases close to 1:4. Higher classification accuracies of 92.8% and 90.3% were observed with ANN and CART, respectively, as compared to the lower classification accuracy of 88.5% with the logistic model. The authors were also able to conclude that the attitude or rationalization of the top management was an extremely important magnitude, besides pressure on management and advantageous opportunity for committing fraud, especially when enormous incidences of financial restatements along with the financial factors could be traced in the records.

Dong et al. (2016) used the SVM model Liblinear to detect financial fraud committed by top firms based on data extracted from the MD&A section of 'Form 10-K', with a sample of 1,610 United States-based companies, of which exactly half were fraudulent. A comparison of the classification accuracy of the method using financial ratios developed by Abbasi et al. (2012) and that of a text detection method utilizing several extraction algorithms to highlight textual features of relevance to classification was done. The average accuracy of the text-based method was found to be 82.36%, which was much better in comparison to the 52.29% achieved by the baseline method. The authors further proceeded to test a model that used both textual features and financial ratios to find an average classification accuracy of 82.49%, which was slightly higher than the stand-alone text-based model, proving that the detection of fraudulent companies can be performed efficiently if the feature set includes both financial ratios and textual information.

Zainuddin and Hashim (2016) conducted a study to analyse the critical financial ratios, including financial leverage, profitability, asset composition, liquidity and capital turnover ratios, in the detection of financial frauds by companies listed in Malaysia. The sample consisted of 30 companies, 15 fraudulent and 15 non-fraudulent, and the period under study was 2007–2013. The fraudulent companies were identified as the ones not meeting the listing requirements as mentioned in Bursa Malaysia Securities. The logistic regression methodology was used to identify the fraudulent firms. However, the study included the fact that the sample size was relatively small and that the companies selected as fraudulent were the ones based on only one criterion, while other firms had been missed out.

Aghghaleh et al. (2016) conducted a study in the Malaysian context to explore the possibility of utilizing the M-score propounded by Beneish (1999) and F-score propounded by Dechow et al. (2011), to enable detection of financial statement frauds while also comparing the accuracy, including the error rates between the two models. The sample included a total of 164 firms, 82 fraudulent and 82 non-fraudulent, from among the Malaysian public listed companies. The period under study was 2000–2014, with financial data collected from Osiris and annual reports. The researchers concluded that the Dechow F-score model outperforms the Beneish M-score model in terms of detection of fraudulent firms with a classification accuracy of 73.17%, as compared to 69.51% for the Beneish model, as well as efficiency in terms of type-II-error percentage, with 26.83% for the Dechow model as compared to 30.49% for the Beneish model. The researchers further recommended that future studies be done for comparing models consisting of both financial and non-financial variables.

Hajek and Henriques (2017) developed a fraud detection system on the basis of financial data and comments noted in the annual reports of 622 companies, consisting of an equal number of fraudulent and non-fraudulent companies, taken from a wide array of sectors. Thirty different sets of data were generated using textual inputs and financial ratios, and 14 different classification techniques were applied on each data set, and the mean of results was computed for each method. The study concluded that the Bayesian belief networks technique, with a classification accuracy of 90.32%, was the best system for classifying non-fraudulent firms. The authors also developed two illustratable Naive Bayes-based models, one with 'green and red flag' values to compute the likelihood of financial fraud and a hybrid model of Naive Bayes and decision tree to classify fraudulent companies. The hybrid model could classify 89.50% cases correctly.

Ines (2017) conducted a study in the French context with a sample of 250 listed French firms, 45 fraudulent and 205 non-fraudulent, with the period of study as 2006–2010, with the objective of exploring the impact of discretionary accruals and governance mechanisms in the occurrence of financial statement fraud. The sample consisted of fraudulent companies identified by the Financial Markets Authority (AMF). The researchers concluded that while aggressive accounting manipulation increases the likelihood of financial statement fraud, conservative accounting policy is negatively associated with corporate fraud.

Pazarskis et al. (2017) conducted a study in the Greek context, specifically during the period of financial crisis (2008–2015) in Greece, with the objective of developing a model for financial statement fraud during the period of turbulence. The sample consisted of companies listed on the Athens Exchange, with 12 firms as the primary research sample wherein financial statement fraud had already been identified. Another set of 12 non-fraudulent companies was selected as the control sample, and the logistic regression methodology was used for the purpose of identifying the fraudulent firms. A classification accuracy of more than 90% was observed, and the researchers concluded that the developed model was effective in detecting fraudulent firms during the period of economic crisis.

Jan (2018) conducted a study in the Taiwanese context for establishing a mechanism to detect financial statement fraud. The sample data consisted of 160 companies, including 40 companies reporting fraudulent financial statements and 120 non-fraudulent companies, listed on the Taiwan/Taipei Exchange. The study was restricted to the financial data pertaining to the period 2004–2014. The researcher conducted a comparative performance analysis by utilizing ANN and SVM in the first stage for feature selection, starting out with 22 variables and reducing the same to significant variables. The researcher then developed four models for classification, namely CART, chi-square automatic interaction detector (CHAID), C5.0 and quick, unbiased, efficient, statistical tree (QUEST). The study indicated that the best classification accuracy of 90.83% for detection of fraudulent firms was observed with the ANN + CART model, which also reported the lowest type-I error (9.79%) and type-II error (8.55%).

Jofre and Gerlach (2018) conducted a detailed study, in the context of United States-based firms, for sector-wise analysis of the implementation of various machine learning–based techniques for detection of accounting fraud. The sample was chosen for a total of 1,594 fraud cases reported in the Accounting Series Releases (ASR) and Accounting and Auditing Enforcement Releases (AAER) issued by the US Securities and Exchange Commission (SEC) between 1990 and 2012. The study used a host of machine learning techniques, and it was observed that a very good classification accuracy was obtained for companies under the categories Agriculture, Forestry and Fishing (although the sample was small) and Public Administration, followed by that for Mining and Construction, while moderate accuracy was observed for companies under Transportation, Communication, Electric, Gas and Sanitary Service and Wholesale Trade and Retail Trade, Finance, Insurance and Real Estate. Poor accuracy was observed for companies under the manufacturing and services categories.

Hajek (2019) used linguistic variables to implement fuzzy rule–based classification schemes for detecting financial statement frauds of US companies. The sample in the study comprised textual information from the annual reports of 622 companies, out of which 311 were fraudulent companies, equally paired with 311 non-fraudulent companies. The feature selection process included an initial feature set of 32 variables. The eight final features were selected using genetic algorithm as a wrapper feature selection method. The researcher used different fuzzy rule–based classification schemes to detect the fraudulent companies and compared the performance of each scheme on the basis of classification accuracy and misclassification cost. The author concluded that with an appropriate methodology for feature selection, even a simple data mining algorithm like fuzzy logic can lead to relatively accurate results of classification of fraudulent companies.

Figure 3 highlights the yearly distribution of the reviewed articles from the year 1995 onwards. It can be observed in Figure 3 that there is an increase in the number of publications since the year 2009 on financial fraud detection. The implementation of machine learning techniques for detection of fraudulent cases has increased since the year 2009.

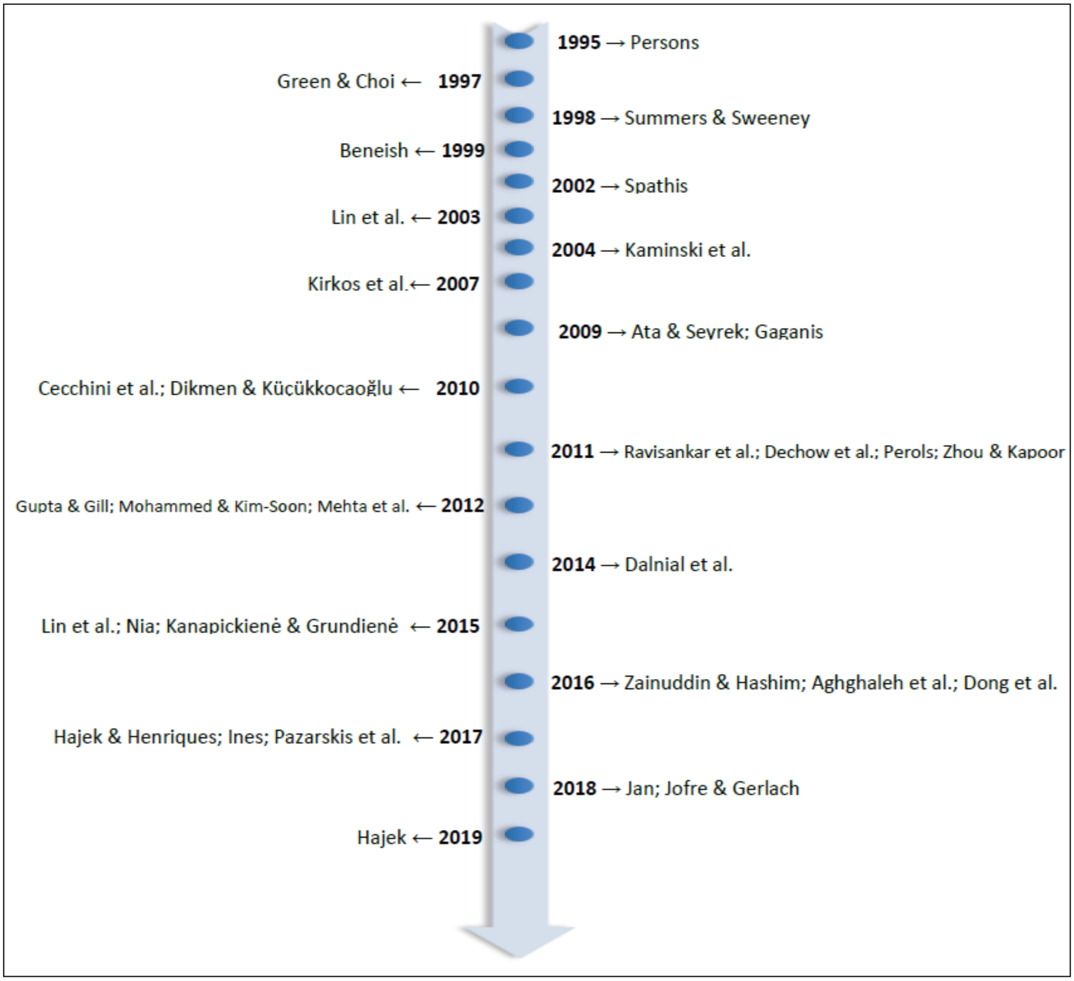
1995 → Persons
Green & Choi ← 1997
1998 → Summers & Sweeney
Beneish ← 1999
2002 → Spathis
Lin et al. ← 2003
2004 → Kaminski et al.
Kirkos et al.← 2007
2009 → Ata & Seyrek; Gaganis
Cecchini et al.; Dikmen & Küçükkocaoğlu ← 2010
2011 → Ravisankar et al.; Dechow et al.; Perols; Zhou & Kapoor
Gupta & Gill; Mohammed & Kim-Soon; Mehta et al. ← 2012
2014 → Dalnial et al.
Lin et al.; Nia; Kanapickienė & Grundienė ← 2015
2016 → Zainuddin & Hashim; Aghghaleh et al.; Dong et al.
Hajek & Henriques; Ines; Pazarskis et al. ← 2017
2018 → Jan; Jofre & Gerlach
Hajek ← 2019

Figure 3. Yearly Distribution of the Reviewed Articles.

Source: The author.

Analysis

Based on the literature review in the context of financial statement fraud detection, the techniques can be classified as univariate techniques and multivariate techniques. These techniques differ on the basis of the model having a single feature or multiple features for classification. Further, the classification analysis for the purpose of fraud detection has been performed using statistical methods or machine learning algorithms. The classification of the data mining techniques, with details of the sample size and classification accuracy of the retrieved studies, are presented in Table 1.

Table 1. Classification Techniques Used to Detect Symptoms of Financial Statement Frauds on the Basis of Sample Size and Overall Accuracy of Classification Techniques.

Sr. No.	Author(s)	Algorithms/Methods Applied	Sample Size	Mapping Ratio	Classification Accuracy (as reported in the literature)
1.	Persons (1995)	Logistic regression	206 firms; 103 fraudulent and 103 non-fraudulent	1:1	71.5%
2.	Green and Choi (1997)	Neural networks	95 firms; 46 fraudulent and 49 non-fraudulent	1:many	71.7%
3.	Summers and Sweeney (1998)	Cascaded logit regression	102 firms; 51 fraudulent and 51 non-fraudulent	1:1	59.8%
4.	Beneish (1999)	Probit regression	2,406 firms; 74 fraudulent and 2,332 non-fraudulent	1:many	89.5%
5.	Feroz et al. (2000)	Neural networks, logistic regression	132 firms; 42 fraudulent and 90 non-fraudulent	1:many	NN: 81% LR: 70%
6.	Spathis (2002)	Logistic regression, univariate and multivariate statistical tools	76 firms; 38 fraudulent and 38 non-fraudulent	1:1	75.4%
7.	Lin et al. (2003)	Logistic regression, neural networks	200 firms; 40 fraudulent and 160 non-fraudulent	1:many	NN: 79% LR: 76%
8.	Kaminski et al. (2004)	Discriminant analysis	158 firms; 79 fraudulent and 79 non-fraudulent	1:1	53.8%
9.	Kirkos et al. (2007)	Decision tree, neural networks and Bayesian belief networks	76 firms; 38 fraudulent and 38 non-fraudulent	1:1	DT: 73.6% NN: 80% BBN: 90.3%
10.	Lenard and Alam. (2009)	Logistic regression	30 firms; 15 fraudulent and 15 non-fraudulent	1:1	77%
11.	Gaganis (2009)	Discriminant analysis (UTADIS), logistic regression, nearest neighbour, artificial neural networks (ANN), probabilistic neural networks (PNN), support vector machines (SVM), univariate and multivariate statistical tools	398 firms; 199 fraudulent and 199 non-fraudulent	1:1	PNN: 82.93% UTADIS: 87.20%

(Table 1 Continued)

(Table 1 Continued)

Sr. No.	Author(s)	Algorithms/Methods Applied	Sample Size	Mapping Ratio	Classification Accuracy (as reported in the literature)
12.	Cecchini et al. (2010)	SVM using custom financial kernel	6,632 firms; 205 fraudulent and 6,427 non-fraudulent	1:many	90.4%
13.	Ravisankar et al. (2011)	PNN in Neuroshell 2.0, genetic programming, logistic regression	202 firms; 101 fraudulent and 101 non-fraudulent	1:1	PNN: 98.09% GP: 94.14% LR: 71%
14.	Dechow et al. (2011)	Logistic regression	79,651 firms; 293 fraudulent and 79,358 non-fraudulent	1:many	63.7%
15.	Mehta et al. (2012)	Logistic regression	60 firms; 30 fraudulent and 30 non-fraudulent	1:1	71.5%
16.	Dalnial et al. (2014)	Multiple linear regression	130 firms; 65 fraudulent and 65 non-fraudulent	1:1	74.7%
17.	Kanapickienė and Grundienė (2015)	Logistic regression	165 firms; 40 fraudulent and 125 non-fraudulent	1:many	64%
18.	Lin et al. (2015)	Logistic regression, decision trees (CART), ANNs	576 cases; 129 fraudulent and 447 non-fraudulent	1:many	LR: 88.5% CART: 90.3% ANNs: 92.8%
19.	Nia (2015)	Mean of financial ratios of fraudulent and non-fraudulent companies; for testing the hypothesis, t-test	134 firms; 67 fraudulent and 67 non-fraudulent	1:1	NA
20.	Aghghaleh et al. (2016)	Beneish and Dechow F-score models for detecting fraud	164 firms; 82 fraudulent and 82 non-fraudulent	1:1	Dechow F-score predicted 73.17% of fraud cases correctly; the Beneish model predicted 69.51% of fraud cases correctly
21.	Dong et al.(2016)	SVM model on textual features extracted from the MD&A section of 'Form 10-K', along with 84 financial ratios	1610 firm-year samples; 805 fraud-year samples and 805 non-fraud-year samples	1:1	82.49%

(Table 1 Continued)

(Table 1 Continued)

Sr. No.	Author(s)	Algorithms/Methods Applied	Sample Size	Mapping Ratio	Classification Accuracy (as reported in the literature)
22.	Zainuddin and Hashim (2016)	Logistic regression	30 firms; 15 fraudulent and 15 non-fraudulent	1:1	73%
23.	Hajek and Henriques (2017)	14 different methods applied on 30 different data sets, logistic regression, Bayesian belief networks, decision table/Naive Bayes (DTNB) hybrid model	622 firms; 311 fraudulent and 311 non-fraudulent	1:1	Mean classification accuracy LR: 74.54% BBN: 90.32% DTNB: 89.50%
24.	Ines (2017)	Pearson's correlation F (*p*-value), adjusted R^2, logistic regression	250 firms; 45 fraudulent and 205 non-fraudulent	1:many	N.A
25.	Pazarskis et al. (2017)	Stepwise logistic regression	24 firms; 12 fraudulent and 12 non-fraudulent	1:1	90.91%
26.	Jan (2018)	ANN + decision tree (CART , CHAID, C5.0, QUEST)	160 firms; 40 fraudulent and 120 non-fraudulent	1:many	CART: 91% CHAID: 90% C5.0: 88% QUEST: 84%
27.	Jofre and Gerlach (2018)	Quadratic discriminant analysis (QDA), logistic regression, AdaBoost decision trees (AB DT), boosted trees (BT) and random forests (RT)	1,594 fraud-year observations till 2012 paired with non-fraud-year observations	1:1	QDA and BT reported as the most accurate models, with both having an accuracy of 87.5%
28.	Hajek (2019)	Fuzzy rule–based system	622 US companies, 311 fraudulent and 311 non-fraudulent, between the years 2005 and 2015	1:1	Accuracy: 86.8% using fuzzy unordered rule induction algorithm (FURIA)

Source: The authors.

The retrieved studies that have used data mining classification techniques for detecting the symptoms of financial statement fraud can be broadly categorized on the basis of the type of techniques applied, as either statistical techniques (Figure 4) or machine learning techniques (Figure 5).

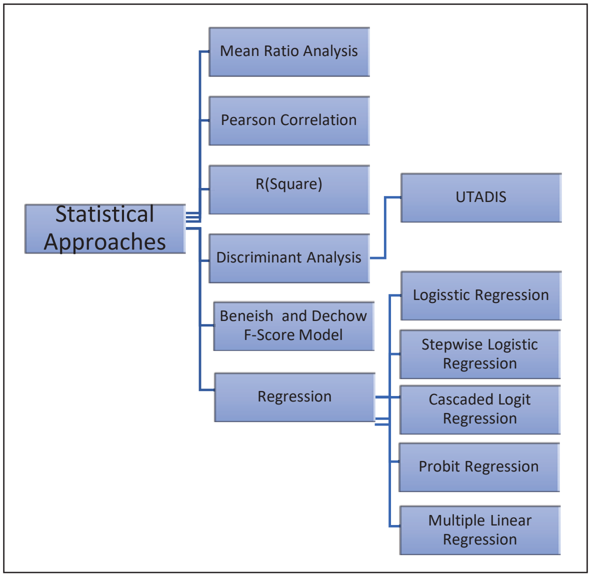

Figure 4. Statistical Approaches Applied for Financial Fraud Detection.

Source: The author.

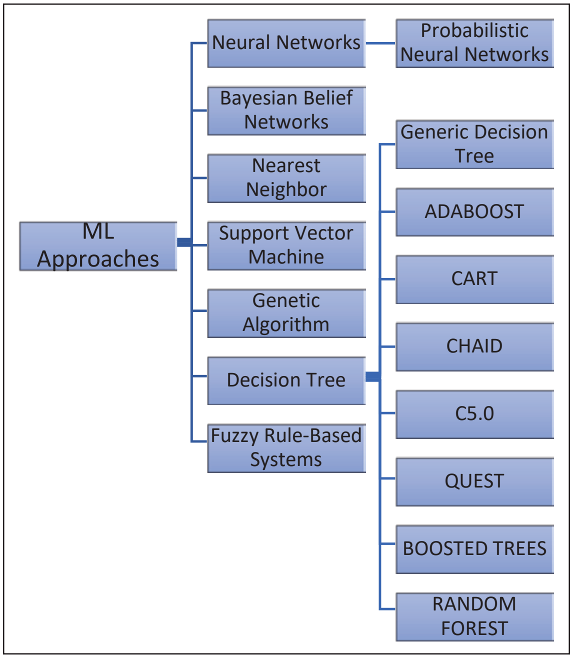

Figure 5. Machine Learning Approaches Applied for Financial Fraud Detection.

Source: The author.

It is observed that the fraud detection techniques mentioned in Figure 3 include statistical tests, such as mean ratio analysis, Pearson's correlation, R^2, discriminant analysis, the Beneish model and the Dechow F-score model. Regression analysis has been extensively used on fraudulence data for classifying linearly separable data sets. The regression models used in the literature include logistic regression, stepwise logistic regression, cascaded logit regression, probit regression, multiple linear regression, et cetera. Variants of discriminant analysis, like UTADIS, have also been used for classification of fraudulent and non-fraudulent companies.

The machine learning approaches such as neural networks and its variant PNN, Bayesian belief networks, the nearest-neighbour framework, SVM, genetic algorithm, decision tree and its variants, such as generic decision tree, AdaBoost, CART, CHAID, C5.0, QUEST, boosted trees, random forests, have been achieving high accuracy in classification results. In a recent study, a fuzzy rule–based system was developed to detect frauds, with textual data taken from the companies' annual reports and auditor's reports (Hajek, 2019).

Figure 6 is a graphical representation of the range of classification accuracy observed with statistical approaches vis-à-vis machine learning approaches, with the classification accuracy obtained from the literature survey summarized in Table 1. The comparison is not point-to-point but is a general indicator of the range of the classification accuracy.

It can be concluded from Figure 6 that, on the whole, the machine learning approaches have outperformed the statistical techniques in terms of overall accuracy of the classification process.

Figure 7 shows the range of overall accuracy percentage achieved using different types of statistical and machine learning approaches where the data mapping ratio is 1:1, that is, where the sample data taken for modelling are for an equal number of fraudulent and non-fraudulent companies. The graph (Figure 7) is not a point-to-point comparison between the statistical and machine learning techniques but is an indicator of the range of the percentage accuracy of the two types of methodologies. It can be observed from the graphical representation that while using the 1:1 data mapping ratio, the overall accuracy achieved by various types of statistical approaches lies in the range of 53%–90%, while that achieved by machine learning approaches lies in the range of 71%–98%.

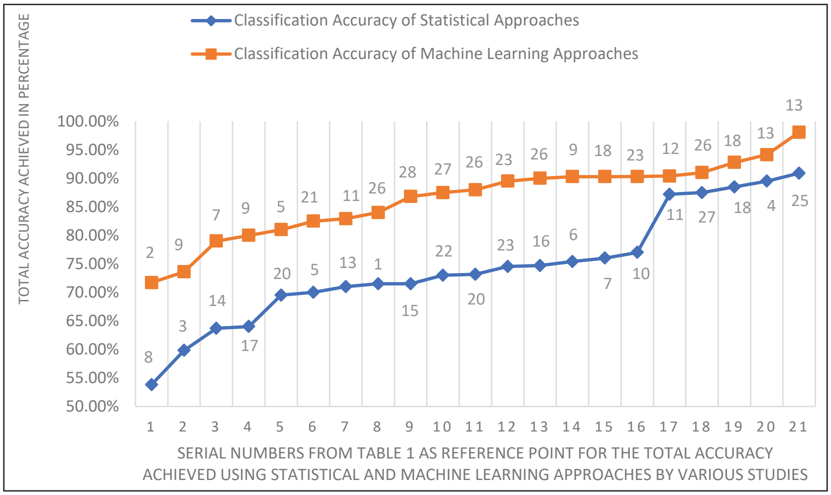

Figure 6. Classification Accuracy of Machine Learning Techniques Versus Statistical Techniques.

Source: The author.

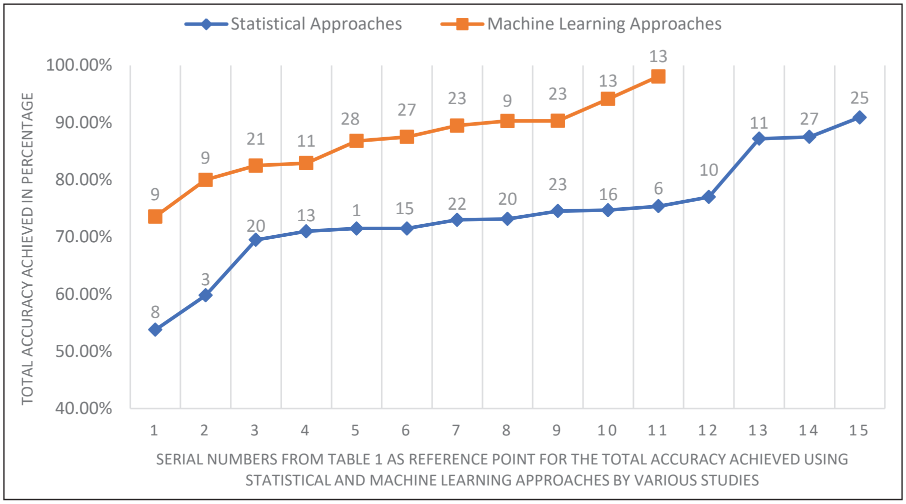

Figure 7. Overall Classification Accuracy (in %) of Machine Learning Techniques Versus Statistical Techniques Achieved with Sample Data Mapping Ratio of 1:1.

Source: The author.

Jofre and Gerlach (2018) (Sr. no. 27 in Table 1), used the statistical classification approach while mapping fraudulent and non-fraudulent companies in 1:1 ratio with a relatively large data sample of 3188 companies but achieved an overall classification accuracy of 87.5 %. On the contrary, the highest overall accuracy of more than 90 % has been achieved by Pazarskis et al. (2017) (Sr. no. 25 in Table 1) who used only 24 companies with 1:1 data mapping and stepwise logistic regression. Further, on comparing the overall classification accuracy achieved by statistical approaches in comparison with machine learning approaches, as presented in figure 6, the highest classification accuracy (89.5 %) was achieved by statistical approach using a data sample comprising of 2,406 firms with 1: Many data mapping ratio, while the highest classification accuracy with machine learning approaches of Ravisankar et al. (2011) (Sr. no. 13 in Table 1) was 98.09 % by using data sample comprising of only 202 firms with 1:1 data mapping ratio.

Figure 8 shows the range of overall accuracy percentage achieved using machine learning approaches, using data sets where the data mapping ratio is 1:1 or 1:many. The graph is not a point-to-point comparison between the different types of data sets but is an indicator of the range of the percentage accuracy of the machine learning approaches with the two types of data sets. Higher accuracy can be observed from the graphical representation (Figure 8) using machine learning approaches where 1:1 mapping is used.

Cecchini et al. (2010), Lin et al. (2015) and Jan (2018) (Sr. nos 12, 18 and 26 in Table 1 as reference points in Figure 8) have classified more than 90% of fraudulent and non-fraudulent companies accurately with a sample data mapping ratio of 1:many and have used 6,633, 576 and 160 companies, respectively, as total data.

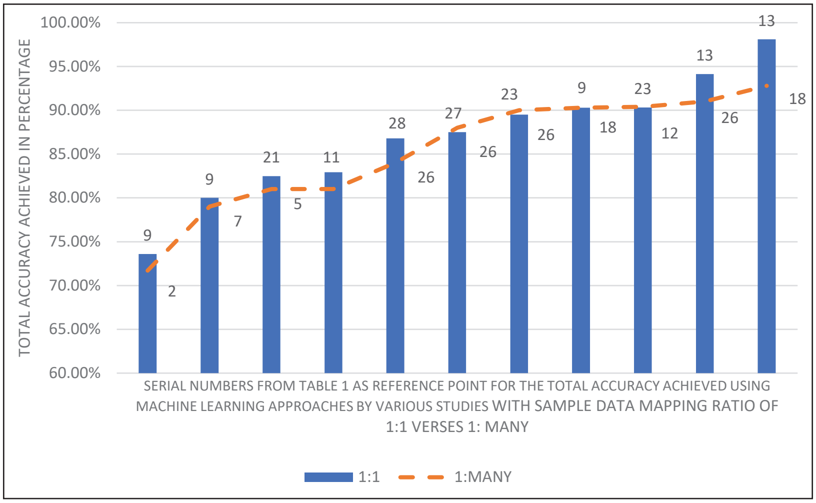

Figure 8. Comparison of Overall Classification Accuracy (in %) of Machine Learning Techniques Achieved with Sample Data Mapping Ratio of 1:1 with 1:Many Sample Data Mapping Ratio.

Source: The author.

The research of Lin et al. (2003), after varying the ratio of the fraudulent to non-fraudulent companies from 1:1 to 1:100, analysing the outcomes of data mining, has concluded that the 1:many mapping ratio results in increased implementation cost of the detection model. The large amount of data would increase the complexity of the model, would also affect the time required for the processes of data collection, data pre-processing and data processing and can increase the overall cost of implementation.

Discussions

The review of the existing academic literature till date reveals that there are two major aspects in financial fraud detection: first, fraudulent sample collection and mapping of fraudulent companies with non-fraudulent companies; and second, selection, application and evaluation of the accuracy of mining techniques in classifying the companies into two broad categories: fraudulent and non-fraudulent.

Through meta-analysis, the supremacy of machine learning methods over statistical approaches is clearly illustrated, both in Figure 6, where no distinction between the 1:1 and 1:many sample mapping cases is made, and in Figure 7, where both approaches are compared in cases where 1:1 sampling is followed. It is also found that implementation of statistical approaches to yield high classification accuracy generally requires an extremely large sample input in both the 1:1 and 1:many mapping approaches, increasing the implementation cost dramatically, though there are some exceptions to it.

To find the superior of the two data sample mapping ratios, the corresponding cases using machine learning, the more accurate method, are compared graphically. It is very apparent that cases utilizing the

1:1 sample mapping outperform/provide more competitive results than those using the 1:many data mapping, making 1:1 the preferable data mapping ratio.

It is also apparent from the analysis that a smaller sample size of fraudulent and non-fraudulent companies mapped using the 1:1 data mapping ratio can increase the efficacy of the model, and most importantly, reduce the time required for the processes of data collection, data pre-processing and data processing. A smaller sample size can further help in reducing the overall cost of implementation.

The review of the academic literature also recommends application of the following commonly used data mining classification techniques for detection of frauds committed through misappropriation or misrepresentation of financial statements: ANN, SVM, decision trees, Bayesian belief networks, genetic algorithms and regression. ANN, Bayesian belief networks and genetic algorithms are very efficient techniques in terms of overall accuracy of the detection process but are also computationally extensive techniques, resulting in slow performance, and involve complex implementation (Rygielski et al., 2002). Similarly, the results achieved with regression or its variants are not very effective in terms of overall accuracy, as shown in Table 1, unless the data set mapping one fraudulent company to many non-fraudulent companies is gigantic, as observed in Beneish (1999). Of these, the most appropriate technique can be selected to suit the needs and objectives of every individual analytical study.

Conclusion

This meta-analysis foremost leads to the conclusion that a 1:1 mapping approach is likely to result in a similar or better range of accuracy as compared to using a large data set with 1:many mapping without increasing the cost of implementation.

This analysis also shows that machine learning methods are more accurate at detecting financial statement frauds than statistical methods, particularly when the availability of sample data is low.

Thus, with the correct choice of a machine learning approach, a high accuracy can be obtained with a 1:1 data mapping set while keeping the overall implementation costs low.

Managerial Implications

The findings of this study have implications for researchers interested in applying machine learning techniques especially in the area of detection of financial statement frauds, where the biggest challenge lies in collecting the sample of fraudulent companies.

Limitations and Future Research

Major research articles published between 1995 and 2019 have been explored for conducting this review. The author has tried to include at least one research article per year on the basis of the citations of these articles. The classification results achieved by the research articles reviewed may also have been impacted by industry type, country, feature set, et cetera.

In this study, the conclusions are drawn about the overall accuracy of data mining techniques. In a future work, the authors intend to perform the comparison based on F-score, which is considered as a measure of testing accuracy through computing the harmonic mean of precision rate and true positive rate.

From the review of the existing literature, it is observed that many researchers have recommended performing feature selection prior to the classification process, which has a positive impact on the accuracy of the classification process. Gupta and Gill (2012) and Nia (2015) have recommended the same. Gupta and Gill (2012), Jan (2018) and Hajek (2019) in their work have reported implementing feature selection using a machine learning technique such as ANN, SVM or decision tree algorithms. Gupta and Mehta (2020) have demonstrated a methodology for feature selection for financial statement fraud detection using a correlation filter–based feature selection algorithm that combines the results of four different machine learning techniques to select a smaller set of features. The influence of feature selection on the classification accuracy of detecting fraudulent cases can be examined, and scope for significant work exists in this direction.

This study can be extended through investigating more articles and analysing the applicability of data mining techniques and data mapping schemes applied, also including the impact of the feature set selected in the domain of financial statement fraud. The findings of this study can also be tested in other domains of data mining.

Acknowledgement

The authors are grateful to the anonymous referees of the journal for their extremely useful suggestions to improve the quality of the article. Usual disclaimers apply.

Declaration of Conflicting Interests

The authors declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

Funding

The authors received no financial support for the research, authorship and/or publication of this article.

References

Abbasi, A., Albrecht, C., Vance, A., & Hansen, J. (2012). Metafraud: A meta-learning framework for detecting financial fraud. *MIS Quarterly, 36*(4), 1293–1327.

Aghghaleh, S. F., Mohamed, Z. M., & Rahmat, M. M. (2016). Detecting financial statement frauds in Malaysia: Comparing the abilities of Beneish and Dechow Models. *Asian Journal of Accounting and Governance, 7*, 57–65.

Agrawal, K., & Chatterjee, C. (2015). Earnings management and financial distress: Evidence from India. *Global Business Review, 16*(5_suppl), 140S–154S.

Altman, E. I., Hartzell, J., & Peck, M. (1998). Emerging market corporate bonds—A scoring system. In R. M. Levich (Ed.), *Emerging Market Capital Flows* (pp. 391–400). Springer.

Ata, H. A., & Seyrek, I. H. (2009). The use of data mining techniques in detecting fraudulent financial statements: An application on manufacturing firms. *Suleyman Demirel University Journal of Faculty of Economics & Administrative Sciences, 14*(2), 157–170.

Beneish, M. D. (1999). The detection of earnings manipulation. *Financial Analysts Journal, 55*(5), 24–36.

Biswas, B., Sengupta, P., & Chatterjee, D. (2020). Examining the determinants of the count of customer reviews in peer-to-peer home-sharing platforms using clustering and count regression techniques. *Decision Support Systems*, 113324. https://doi.org/10.1016/j.dss.2020.113324

Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical Science,* 235–249.

Cecchini, M., Aytug, H., Koehler, G. J., & Pathak, P. (2010). Detecting management fraud in public companies. *Management Science, 56*(7), 1146–1160.

Coderre, D. G. (1999). *Fraud detection: Using data analysis techniques to detect fraud*. Global Audit Publications.

Dalnial, H., Kamaluddin, A., Sanusi, Z. M., & Khairuddin, K. S. (2014). Detecting fraudulent financial reporting through financial statement analysis. *Journal of Advanced Management Science, 2*(1), 17–22.

Das, R. C., Mishra, C. S., & Rajib, P. (2018). Firm-specific parameters and earnings management: A study in the Indian context. *Global Business Review, 19*(5), 1240–1260.

Dechow, P. M., Ge, W., Larson, C. R., & Sloan, R. G. (2011). Predicting material accounting misstatements. *Contemporary Accounting Research, 28*(1), 17–82.

Dikmen, B., & Küçükkocaoğlu, G. (2010). The detection of earnings manipulation: The three-phase cutting plane algorithm using mathematical programming. *Journal of Forecasting, 29*(5), 442–466.

Dong, W., Liao, S., & Liang, L. (2016). *Financial statement fraud detection using text mining: A systemic functional linguistics theory perspective*. In Pacific Asia Conference on Information Systems (PACIS), Association for Information System. PACIS 2016 Proceedings. 188. http://aisel.aisnet.org/pacis2016/188

Fanning, K. M., & Cogger, K. O. (1998). Neural network detection of management fraud using published financial data. *Intelligent Systems in Accounting, Finance & Management, 7*(1), 21–41.

Feroz, E. H., Kwon, T. M., Pastena, V. S., & Park, K. (2000). The efficacy of red flags in predicting the SEC's targets: An artificial neural networks approach. *Intelligent Systems in Accounting, Finance & Management, 9*(3), 145–157.

Gaganis, C. (2009). Classification techniques for the identification of falsified financial statements: A comparative analysis. *Intelligent Systems in Accounting, Finance & Management: International Journal, 16*(3), 207–229.

Gray, G. L., & Debreceny, R. S. (2014). A taxonomy to guide research on the application of data mining to fraud detection in financial statement audits. *International Journal of Accounting Information Systems, 15*(4), 357–380.

Green, B. P., & Choi, J. H. (1997). Assessing the risk of management fraud through neural network technology. *Auditing, 16*, 14–28.

Gupta, R., & Gill, N. S. (2012). Prevention and detection of financial statement fraud–An implementation of data mining framework. *Editorial Preface, 3*(8), 150–160.

Gupta, S., & Mehta, S. K. (2020). Feature selection for dimension reduction of financial data for detection of financial statement frauds in context to Indian Companies. *Global Business Review*. https://doi.org/10.1177/0972150920928663

Hajek, P. (2019, May). *Interpretable fuzzy rule-based systems for detecting financial statement fraud*. In IFIP International Conference on Artificial Intelligence Applications and Innovations, pp. 425–436, Springer.

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

Han, J., Pei, J., & Kamber, M. (2011). Data mining trends and research frontiers. In J. Han, J. Pei, & M. Kamber (Eds.), *Data mining: Concepts and techniques* (3rd ed., Vol. 560, pp. 499–502). Morgan Kaufmann. https://d1wqtxts1xzle7.cloudfront.net/43034828/Data_Mining_Concepts_And_Techniques_3rd_Edition.pdf

Ines, A. M. A. R. A. (2017). The effect of discretionary accruals on financial statement fraud: The case of the French Companies. *International Research Journal of Finance and Economics, May*(161), 48–62.

Jan, C. L. (2018). An effective financial statements fraud detection model for the sustainable development of financial markets: Evidence from Taiwan. *Sustainability, 10*(2), 513.

Jofre, M., & Gerlach, R. H. (2018). *Fighting accounting fraud through forensic data analytics*. https://www.researchgate.net/publication/325033608_Fighting_Accounting_Fraud_Through_Forensic_Data_Analytics

Kaminski, K. A., Wetzel, T. S., & Guan, L. (2004). Can financial ratios detect fraudulent financial reporting? *Managerial Auditing Journal, 19*(1), 15–28.

Kanapickienė, R., & Grundienė, Ž. (2015). The model of fraud detection in financial statements by means of financial ratios. *Procedia-Social and Behavioral Sciences, 213*, 321–327.

Kirkos, E., Spathis, C., & Manolopoulos, Y. (2007). Data mining techniques for the detection of fraudulent financial statements. *Expert Systems with Applications, 32*(4), 995–1003.

Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering–A systematic literature review. *Information and Software Technology, 51*(1), 7–15.

Kotsiantis, S., Koumanakos, E., Tzelepis, D., & Tampakas, V. (2006). Forecasting fraudulent financial statements using data mining. *International Journal of Computational Intelligence, 3*(2), 104–110.

Kumar, R., & Verma, R. (2012). Classification algorithms for data mining: A survey. *International Journal of Innovations in Engineering and Technology (IJIET), 1*(2), 7–14.

Lenard, M. J., & Alam, P. (2009). An historical perspective on fraud detection: From bankruptcy models to most effective indicators of fraud in recent incidents. *Journal of Forensic & Investigative Accounting, 1*(1), 1–27.

Lin, J. W., Hwang, M. I., & Becker, J. D. (2003). A fuzzy neural network for assessing the risk of fraudulent financial reporting. *Managerial Auditing Journal, 18*(8), 657–665.

Lin, C. C., Chiu, A. A., Huang, S. Y., & Yen, D. C. (2015). Detecting the financial statement fraud: The analysis of the differences between data mining techniques and experts' judgments. *Knowledge-Based Systems, 89*, 459–470.

Mehta, U., Patel, A., Patel, H., & Purohit, R., (2012, January–June). *Detection of fraudulent financial statement in India: An exploratory study.* In Proceedings of the 2nd International Conference on Enterprise Systems & Accounting (ICESA 2005), GFMJR, Vol. 4.

Mohammed, A. A. E., & Kim-Soon, N. (2012). Using Altman's model and current ratio to assess the financial status of companies quoted in the Malaysian stock exchange. *International Journal of Scientific and Research Publications, 2*(7), 1–11.

Ngai, E. W., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems, 50*(3), 559–569.

Nia, S. H. (2015). Financial ratios between fraudulent and non-fraudulent firms: Evidence from Tehran Stock Exchange. *Journal of Accounting and Taxation, 7*(3), 38–44.

Pazarskis, M., Drogalas, G., & Baltzi, K. (2017). Detecting false financial statements: Evidence from Greece in the period of economic crisis. *Investment Management and Financial Innovations, 14*(3), 102–112.

Perols, J. (2011). Financial statement fraud detection: An analysis of statistical and machine learning algorithms. *Auditing: A Journal of Practice & Theory, 30*(2), 19–50.

Persons, O. S. (1995). Using financial statement data to identify factors associated with fraudulent financial reporting. *Journal of Applied Business Research, 11*, 38–38.

Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). *A comprehensive survey of data mining-based fraud detection research* (pp. 1–14). https://arxiv.org/ftp/arxiv/papers/1009/1009.6119.pdf

Phyu, T. N. (2009, March). *Survey of classification techniques in data mining*. In Proceedings of the International MultiConference of Engineers and Computer Scientists, Vol. 1, pp. 18–20. http://www.iaeng.org/publication/IMECS2009/IMECS2009_pp727-731.pdf

Rahman, R. M., & Afroz, F. (2013). Comparison of various classification techniques using different data mining tools for diabetes diagnosis. *Journal of Software Engineering and Applications, 6*(3), 85.

Ravisankar, P., Ravi, V., Rao, G. R., & Bose, I. (2011). Detection of financial statement fraud and feature selection using data mining techniques. *Decision Support Systems, 50*(2), 491–500.

Rezaee, Z., & Riley, R. (2009). *Financial statement fraud: Prevention and detection* (2nd ed.). John Wiley & Sons.

Rygielski, C., Wang, J. C., & Yen, D. C. (2002). Data mining techniques for customer relationship management. *Technology in Society, 24*(4), 483–502.

Spathis, C. T. (2002). Detecting false financial statements using published data: Some evidence from Greece. *Managerial Auditing Journal, 17*(4), 179–191.

Summers, S. L., & Sweeney, J. T. (1998). Fraudulently misstated financial statements and insider trading: An empirical analysis. *Accounting Review, 73*(1), 131–146.

Yamanishi, K., Takeuchi, J. I., Williams, G., & Milne, P. (2004). On-line unsupervised outlier detection using finite mixtures with discounting learning algorithms. *Data Mining and Knowledge Discovery, 8*(3), 275–300.

Yue, D., Wu, X., Wang, Y., Li, Y., & Chu, C. H. (2007, September). *A review of data mining-based financial fraud detection research*. In Proceedings of the 2007 International Conference on Wireless Communications, Networking and Mobile Computing (pp. 5519–5522). IEEE Computer Society. http://www.iaeng.org/publication/IMECS2009/IMECS2009_pp727-731.pdf

Zainuddin, E. F., & Hashim, H. A. (2016). Detecting fraudulent financial reporting using financial ratio. *Journal of Financial Reporting and Accounting, 15*, 266–278.

Zhang, D., & Zhou, L. (2004). Discovering golden nuggets: Data mining in financial application. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 34*(4), 513–522.

Zhou, W., & Kapoor, G. (2011). Detecting evolutionary financial statement fraud. *Decision Support Systems, 50*(3), 570–575.