BMIJ
ISSN: 2148-2586

bmij (2023) 11 (2):451-467

doi: https://doi.org/10.15295/bmij.v11i2.2200

Research Article

Detection of fraudulent transactions using artificial neural networks and decision tree methods

Yapay sinir ağları ve karar ağacı yöntemleri kullanılarak hileli işlemlerin tespiti

Yusuf Işık[1]

İlker Kefe[2]

Jale Sağlar[3]

[1] Dr. Instructor, Hatay Mustafa Kemal University, Hatay, Türkiye, yusufisik@mku.edu.tr

ORCID: 0000-0001-5842-4365

[2] Asst. Prof., Osmaniye Korkut Ata University, Osmaniye, Türkiye, ilkerkefe@osmaniye.edu.tr

ORCID: 0000-0002-9945-5325

[3] Assoc. Prof., Cukurova University, Adana, Türkiye, jsaglar@cu.edu.tr

ORCID: 0000-0001-7152-9807

Corresponding Author:

İlker Kefe,

Osmaniye Korkut Ata University, Osmaniye, Türkiye, ilkerkefe@osmaniye.edu.tr

Abstract

The accounting systems generate a large amount of data due to financial transactions. Intentionally fraudulent transactions can occur in high-dimensional and large numbers of emerging data. While many methods can be used for the estimation and detection of fraudulent transactions in accounting, which differ in the audit process, scope and application method, data mining methods can also be used today due to a large number of data and the desire not to narrow the scope of the audit. This study tested the accuracy of detecting fraudulent transactions using artificial neural networks and decision tree methods. According to the results of the analysis test data set for detecting fraud or error risk, 99.7981% accuracy was obtained in the artificial neural networks method and 99.9899% in the decision tree method.

Keywords: Data Mining, Accounting, Fraud Detection, Artificial Neural Networks, Decision Tree

Jel Codes: M42, C49

Öz

Muhasebe sistemleri, finansal işlemler nedeniyle büyük miktarda veri üretir. Ortaya çıkan yüksek boyutlu ve çok sayıdaki bu verilerde bilerek hileli işlemler gerçekleşebilir. Muhasebede hileli işlemlerin tahmini ve tespiti için denetim süreci, kapsamı, uygulanma metodu farklılık gösteren birçok yöntem kullanılabilmekteyken günümüzde veri sayısının çok fazla olması ve denetim kapsamını daraltmama isteği gibi sebeplerle veri madenciliği yöntemleri de kullanılabilmektedir. Bu çalışmada yapay sinir ağları ve karar ağacı yöntemleri kullanılarak hileli işlemlerin tespitinin doğruluğu test edilmiştir. Hile veya hata riskinin tespiti için yapılan analiz test veri seti sonuçlarına göre yapay sinir ağları yönteminde %99.7981, karar ağacı yönteminde %99.9899 doğruluk elde edilmiştir.

Anahtar Kelimeler: Veri Madenciliği, Muhasebe, Hile Tespiti, Yapay Sinir Ağları, Karar Ağacı

JEL Kodları: M42, C49

Submitted: 12/01/2023

Revised: 22/02/2023

Accepted: 31/03/2023

Online Published: 26/06/2023

Citation: Işık, Y., Kefe, İ., & Sağlar, J., Detection of fraudulent transactions using artificial neural networks and decision tree methods, bmij (2023) 11 (2): 451-467, doi: https://doi.org/10.15295/bmij.v11i2.2200

Introduction

Accounting, as a discipline and a business function, provides a system in which economic data is processed, and the processed data is turned into cumulative information, summarized, and reported (Kıymetli Şen & Terzi, 2022). Businesses need accounting to perform "internal and external reporting, costing, forecasting, evaluation, analysis, and auditing". Numerous of these functions involve significant levels of unpredictability and risk (Amani & Fadlalla, 2017). One of the most frequently debated topics in the accounting literature is fraud, one of these unpredictable and risky elements. As a result, accounting professionals now have a crucial task: identifying financial fraud (Tang & Karim, 2019). Fraud is one of the most costly and common forms of financial crime worldwide. Fraud refers to fraudulent acts committed by individuals against the organizations that employ them (ACFE Report, 2022). According to the Association of Certified Fraud Examiners (ACFE), financial statement fraud is "The intentional misstatement or omission of material facts, or accounting data which is misleading and, when considered with all the information made available, would cause the reader to change or alter his or her judgment or decision." (Zhou & Kapoor, 2011). Fraud detection has drawn significant attention from scholars and businesses worldwide, resulting from its rising popularity (Kotekani & Velchamy, 2020). Every fraudulent act has a cost to businesses. While the cost of detected and reported fraudulent transactions can be calculated, the cost of fraudulent transactions that cannot be detected remains an economic loss forever (Kılıç & Önal, 2021). Identifying fraudulent activity is becoming increasingly crucial due to the growing number of reported fraud instances and the harm it brings to businesses and investors (Ata & Seyrek, 2009). The research conducted by ACFE in 2022, by considering 2.110 cases in 133 countries, and 23 industries, determined that a total loss of more than 3.6 billion dollars was caused due to fraudulent transactions. The ACFE report highlighted that Certified Fraud Examiners (CFE) estimate that businesses lose 5% of their annual revenue due to fraudulent transactions.

Good accounting practices have been used for over 40 years (Baldwin, Brown & Trinkle, 2006). It may be said that since its characterization of unpredictability and variability, fraud detection turns into hard work involving both expertise and technology (Tang & Karim, 2019). Using data analytics for fraud detection is common (Debreceny & Gray, 2010). Though the studies combine data and technology, which offers great help to the research on fraud detection methods, they still dismiss non-numerical indications from those who make prepared financial statements (Tang & Karim, 2019). Its massive size due to skewed distributions and excessive scales characterize datasets. When evaluating datasets, skewed class distribution and its size are regarded as serious challenges since they raise the rate of "misclassification" (Kotekani & Velchamy, 2020). Advances in information technologies and digitization have contributed to the frequent use of computer software, machine learning algorithms, and artificial intelligence. The processes of producing, storing, analyzing, and transmitting information to relevant parties have accelerated and changed (Kıymetli Şen & Terzi, 2022). The main purpose of applying data mining is the effective use of an organization's data assets for economic or non-economic outcomes. Hence, practically all business and non-business professions, including accounting, have used data mining (Amani & Fadlalla, 2017). Data mining techniques, which assert to have sophisticated categorization and prediction capacities, may make it easier for auditors to discover fraud detection (Kirkos, Spathis & Manolopoulos, 2007).

A purposeful provision of misleading information in a financial statement constitutes fraud, which is now a serious economic and social issue (Zhou & Kapoor, 2011). Financial statement fraud is directly tied to bookkeeping and daily operations because it involves the deliberate manipulation of financial records, improper implementation of accounting rules, financial performance, and other behaviours that produce ambiguity (Rezaee, 2005). Using data mining methods to identify characteristics from journal entries to spot fraud is one way to figure out a financial statement fraud (Debreceny & Gray, 2010). Financial restatements frequently occur because of mistakes and misrepresentations in accounting records (Tang & Karim, 2019).

The indicators of accounting and information systems rarely match fraud prediction. This difference is because accounting is more field-oriented and based on historical data. At the same time, information systems are more process-oriented, focusing on improving the results of the fraud detection model with innovative business analytics techniques (Albizri, Appelbaum & Rizzotto, 2019). There is an extensive literature review on the important data mining paradigm in accounting but applied research that provides a holistic view of these uses is lacking. This study tests two Data Mining (DM) techniques for their applicability in fraud detection: decision trees and artificial neural networks. This article proceeds as follows: In the second section, we first discuss data mining in fraud detection and the method used to collect and analyze the financial statements fraud detection literature. In the third and fourth sections, we review the application of decision trees and artificial neural networks. In the fifth section, we provide the results of our analysis, including the comparison of decision trees and artificial neural networks, the analysis of the techniques employed, and the analysis of algorithms applied. The sixth section gives the analysis results made with artificial neural networks and decision tree methods. The final section provides concluding.

Data mining in fraud detection

Investors, board directors, auditors, governments, and regulators who ensure the financial safety and long-term viability of the economy must pay attention to fraud detection techniques (Ugrin & Odom, 2010). Detection of fraud earlier, reaching those responsible more quickly, and making necessary interventions before reaching irreparable or impossible dimensions are factors in the possible costs that may arise due to fraud (Önal & Kılıç, 2019). Conducting an integrative and comprehensive review of financial statement fraud detection research is badly needed since there is continual attention from the industry, the public, and the government. Combining the results from many areas may increase the impact of fraud detection operations and research (Albizri et al., 2019). The following tactics could be used in financial fraud: (1) falsification, modification, or manipulation of significant financial records, documentation, or commercial activities; (2) substantial intentional falsifications, inaccuracies, or misleading statements of facts or other significant data used in the preparation of financial statements; (3) improper implementation of accounting rules, principles, practices, and procedures used to measure, identify, and record economic events and commercial activities; (4) the deliberate withholding of information on accounting requirements, guidelines, and processes, as well as the presentation of insufficient disclosures; (5) the application of aggressive belligerent accounting methods through unethical earnings management; (6) manipulation of accounting procedures under the current rules-based accounting standards, which have grown too complex, too simple to work around, and contain vulnerabilities that permit businesses to conceal the economic basis of their achievement (Rezaee, 2005).

In recent years, many researchers have investigated the application of data mining in accounting (Amani & Fadlalla, 2017). Ata and Seyrek (2000) used data mining techniques to help detect fraud in financial statements. They stated that financial ratios such as leverage and return on assets are used to detect fraud. Yang (2006) pointed out how data mining is useful in auditing and fraud detection. Liou (2008) conducted a study comparing fraudulent financial reporting detection models and business failure prediction models. The study utilized various data mining algorithms, including logistic regression, neural networks, and decision trees. Ata and Seyrek (2009) analyzed the financial statements of companies traded in the Istanbul Stock Exchange (ISE) and operating in the manufacturing sector for fraud detection. Seyrek and Ata (2010) measured the efficiency of deposit banks operating in the Turkish banking sector using the data envelopment analysis (DEA) method. Then, using the efficiency scores of the banks, the financial performance indicators that are important in estimating the bank's efficiency were determined using data mining techniques. Ngai, Hu, Wong, Chen and Sun (2011) explored the application of data mining techniques to detect financial fraud and mentioned that data mining techniques used for fraud detection provided immediate solutions to the problems inherent in detecting and classifying fraudulent data. Kıymetli Şen and Terzi (2012) examined the use of data mining in detecting falsified financial statements of companies traded in the financial sector on the ISE. Kılıç and Seyrek (2012) applied artificial neural networks, one of the data mining methods, to determine the factors for estimating financial failures of companies traded in the ISE and operating in the manufacturing sector. Terzi (2012) examined the data mining methods used in the accounting audit and explained which data mining methods/activities will be used at which stage of the audit process. Dayı and Ata (2012) used the data mining method due to the limited number of studies in which financial ratios, economic indicators and stock market performance information were used together. The study used the artificial neural networks method to predict the stock returns of a manufacturing company traded in the ISE. Terzi and Kıymetli Şen (2012) conducted empirical research on manufacturing companies listed on the Istanbul Stock Exchange using data mining classification methods. The study aims to detect fraudulent financial statements with the help of data mining. Gray and Debreceny (2014) ensured a taxonomy to guide research on the application of data mining to fraud detection in financial statement audits. Terzi and Kıymetli Şen (2015) used the artificial neural network model, one of the data mining methods, to detect fraud in forensic accounting. Amani and Fadlalla (2017) reviewed data mining applications in accounting. They determined that the accounting fields most benefited from data mining were fraud detection, assurance and compliance, business health, and forensic accounting. Yao, Zhang, and Wang (2018) proposed an optimized financial fraud detection model combining feature selection and machine learning classification. Factors affecting fraud behaviour were also calculated and analyzed in the study. Jan (2018) aimed to establish an effective model to detect financial statement fraud in enterprises using data mining techniques. Kopun (2018) examined previous research on data mining methods to detect financial statement fraud, focusing on financial analysis indicators that can detect fraud in financial statements. Ye, Xiang, and Gan (2019) investigated the use of data mining techniques such as Random Forest (RF), Artificial Neural Networks (ANNs), Logistics Regression (LR), Support Vector Machine (SVM), Decision Tree (DT), and Bayesian Networks (BN) in detecting financial statement fraud using published financial disclosures. Aksoy (2021), in the research conducted on companies traded in Borsa Istanbul, used a model created to predict financial statement fraud in companies one year in advance using data mining. Kırda and Katkat Özçelik (2021) conducted research to identify companies that are at risk of financial statement fraud with K-Nearest Neighbor (KNN), Random Forest (RF), and XGBoost (XGB), which are classification methods of data mining. Tatar and Kıymık (2021) examined the financial statements of companies traded in the textile, clothing and leather sectors in Borsa Istanbul. They investigated the detection of fraud risk through financial ratios using data mining methods and the success of these methods in detecting fraud. Kılıç and Önal (2022) developed a model to predict the detection of financial statement fraud based on the financial data of companies in Borsa Istanbul in the BIST Watchlist, BIST Stars, and BIST Main Market groups between 2012 and 2019. As a result, many academics, practitioners, and regulators have attempted to develop automated fraud detection tools and techniques (Albizri et al., 2019).

Because fraudsters' actions, bonuses, and strategies are unpredictable and uncertain, fraud detection necessitates a skill set that includes diligence and judgment (Tang & Karim, 2019). One of the most important current concepts of innovative, sophisticated business analytics and predictive modelling instrument is DM (Amani & Fadlalla, 2017). By employing DM techniques, auditors might better detect fraud (Kirkos et al., 2007). DM can be explained that certain algorithms being put into service to "extract patterns from data" (Amani & Fadlalla, 2017). DM is frequently used to extract and reveal the hidden realities underlying huge quantities of data, making it a crucial tool for financial fraud detection (Ngai et al., 2011).

The use of data mining in auditing is currently in its infancy, and researchers approach the subject randomly, looking for patterns in the disclosures made in financial statements, the text of annual reports, and the nature of journal entries without properly applying the lessons learned from previously observed fraud patterns (Gray & Debreceny, 2014). Analytics might offer a more thorough and effective investigation of fraud. Efficient scanning of a whole database and selecting those activities that require further extensive testing seems achievable using the most recent analytical tools, modern ERP systems, and databases (Albizri et al., 2019). Audit companies and their procedures are insufficient to detect and prevent fraud and irregularities in companies. In particular, standard audit procedures in audit companies are not sufficient to detect fraud and irregularities in most cases (Terzi, 2012). In addition to traditional auditing methods, more successful models can be created with new auditing applications developed by using technological opportunities (Kılıç & Önal, 2021). DM techniques are widely used in accounting auditing because they contain less margin of error than other methods (Ulucan Özkul & Pektekin, 2009). DM methods in identifying financial statement frauds in businesses with large volumes of data will provide time and cost benefits in identifying unusual transactions and financial statement frauds (Terzi & Kıymetli Şen, 2015).

Characterized by data mining, researchers have explored numerous methods and used them to identify fraud, including decision trees and neural networks (Kirkos et al., 2007). It has been demonstrated that these methods work well in the beginning. However, the best data features and detection methods are not universally agreed upon. Additionally, although guided approaches have been among the most widely used techniques for identifying financial statement fraud, most corresponding applications do not maintain pace with new techniques created specifically for fraud. In addition, new forms of financial fraud are getting harder and harder to catch with the help of available detection methods (Zhou & Kapoor, 2011). A model for classifying fraud using Neural Networks was created by Green and Choi in 1997. The outcomes demonstrated the enormous potential of neural networks as a fraud detection instrument. A neural network was utilized by Fanning and Cogger (1998) to create a fraud detection system. Kirkos et al. (2007) examined the effectiveness of Decision Trees, Neural Networks and Bayesian Belief Networks in detecting false financial statements. The decision tree and neural network models had high accuracy of 73.6% and 80%, respectively. Artificial neural networks (ANNs) and decision trees (DT) were utilized by Lin, Chiu, Huang and Yen (2015) to identify financial statement fraud. To evaluate the machine learning expert system that predicted the presence of fraud, the study chose 129 fraud cases and 447 non-fraud cases. Using training and testing samples, the ANNs and DT techniques successfully classify objects with correct classification ratios of 91.2% (ANNs) and 90.4% (DT) and 92.8% (ANNs) and 90.3% (DT), respectively. Support Vector Machine (SVM), Random-Forest (RF), Decision Tree (DT), K-Nearest Neighbor (KNN), Linear Regression (LR), Nave Bayes (NB), and Multi-Layer Perceptron (MLP) are some of the classification algorithms that Rukhsar, Bangyal, Nisar and Nisar (2022) compared to identify fraud. According to comparisons of classification algorithms, DT provides the best accuracy of 79% when compared to other methods. Four alternative classification techniques were utilized by Kotekani and Velchamy (2020): Logistic Regression, DT, KNN, and ANNs. Among the classifiers, ANNs had the greatest F1-score of 98.9% and the quickest implementation time delay.

DT and ANNs, data mining methods, come to the fore in studies for detecting fraudulent transactions. Gür (2023) detected fraud using the DT method with an artificial data set that includes normal transactions and fraudulent transactions belonging to a bank. Rukhsar et al. (2022) used the DT method to predict insurance fraud detection. Gür and Tarhan Mengi (2022) used DT, SVM, Logistic Regression, and ANNs methods to detect fraud, and it was determined that the most accurate prediction model was created by the DT method. Kılıç and Önal (2022), Kara and Özcan (2020), Terzi and Kıymetli Şen (2012) used ANNs data mining method. Uğurlu and Sevim (2015) concluded that the ANNs model predicts more successfully than other models in estimating fraudulent financial statements. Kotekani and Velchamy (2020) emphasized that the most accurate result is achieved in ANNs among Logistic Regression, DT, KNN, and ANNs methods. DT and ANNs methods have been used together in many studies (Kirkos, Spathis & Manolopoulos, 2008; Kirkos et al., 2007; Ata & Seyrek, 2009; Ngai et al., 2011; Zhou & Kapoor, 2011; Terzi & Kıymetli Şen, 2012; Kıymetli Şen & Terzi, 2012; Lin et al., 2015; Dutta, Dutta & Raahemii, 2017). Therefore, in this study, artificial neural networks and decision tree methods were implemented using a business's data.

Decision tree (DT)

By grouping cases according to attribute values, DT is a tree that categorizes cases. Each node reflects an attribute in a classification instance in a decision tree, and a node's possible values are symbolized by each branch (Kotsiantis, Koumanakos, Tzelepis & Tampakas, 2006). There is a hierarchical formation with many branches in DT in a characteristic manner: a root node (the top of the tree), an internal node, and a leaf node (the bottom part). If-Then expressions serve as the foundation for a decision tree output. Four components (f1, f2, f3, and f4) and a target are included in a transactional dataset (fraud and non-fraud). In 2020, Kotekani and Velchamy concluded that the resulting measurements depended on a certain query that could assist them in obtaining the desired variable. According to Tang, Liu, Yang and Wei (2018), tree forms in DT begin with only one root node. Every node symbolizes a test on an attribute, and every branch reflects the test's result (Kirkos et al., 2007).

The tree's leaf nodes keep track of some class-label values that point to potential classification outcomes (Tang et al., 2018). The tree makes an effort to separate findings into reciprocally unique subcategories. The choice of the attribute that best sets apart the sample determines the quality of a separation (Kirkos et al., 2007). A route from the root node to the leaf node produces a classification rule, and a decision tree can be converted into several classification rules effortlessly (Tang et al., 2018). Findings are released in the shape of a tree with the help of DT. While leaves are identified with classes in the DT, internal nodes display the properties meaningfully. DT is constructed upside-down, and the root node turns into the top node. They are frequently employed in data mining because of their reliability and simplicity. DT chooses the best feature that provides the most data for the categorization. The classifier stops when all leaf nodes have become pure (Rukhsar et al., 2022).

Artificial neural networks (ANNs)

In an effort to find hidden links in data, ANNs are characterized as a collection of algorithms that employ methods resembling those of the human brain (Mururunkwere, Tuyishimire, Haughton & Nzabanita, 2022). A whole family of structures known as ANNs are used in machine learning and are designed to mimic how the human brain utilizes interlinked neurons to make decisions (Kotekani & Velchamy, 2020). As a result, several neurons, or interlinked processing elements, make up ANNs. Each link has a weight, or numerical value, attached (Kirkos et al., 2007).

The number of layers varies according to the type of ANNs (Kirkos et al., 2007). The nearby nodes of each layer are connected. Pérez López, Delgado Rodríguez and de Lucas Santos (2019) stated that the input layer, where data is supplied to the network, comprises input nodes that directly accept the information from the outside world. Each neuron takes signals from associated neurons, and the sum of those signals is determined as the input signal (Kirkos et al., 2007).

Neurons which have tied to an input layer have a corresponding weight. The input layer and its weight will be conveyed to the hidden layer together (Kotekani & Velchamy, 2020). By sending the information out, the output layer shows how the network has responded to its received inputs. The only layers with no link to the outside are the hidden or intermediate layers, which are situated between the input and output layers and process the information (Pérez López et al., 2019). Processing elements known as neurons and nodes make up a neural network. Layers are the groups that nodes are put in.

A neural network is an input, output, and hidden layered tree-like structure (Kotekani & Velchamy, 2020). Pérez López et al. (2019) stated that there are typically three layers: an input layer, one or more hidden layers, and an output layer. Neurons are shaped like layers. At the very least, a layered network must have an input (first) and an output (final) layer. There may be one or more hidden layers between the input and output. Numerous units (neurons) are connected in a pattern to form a multi-layer neural network. The network must first undergo training, testing, or familiarization. To establish the input-output mapping on a collection of paired data. After setting the weights of the connections between neurons, an entirely new set of data is classified using the network (Kotsiantis et al., 2006). Following the definition of the network architecture, the network needs to be taught after the network architecture has been established. Backpropagation networks compute the final output at the output layer after applying a pattern to the input layer. By adjusting the connection weights, errors in the output are transmitted backwards in the ANNs and compared to the desired outcome. This procedure repeats continuously until a tolerable error rate is obtained (Kirkos et al., 2007). ANNs are widely used in the financial industry, marketing, forecasting, and more frequently in risk assessment and fraud detection because they make it simple to manage larger datasets and, despite their sophisticated algorithms, they produce findings that are simple to illustrate (Murorunkwere et al., 2022).

Data and methods

In this study, 6-month of data on a sportswear business, the leader in the clothing market and one of the highest-ranked distributors in Turkey for a particular product were analysed. Using 502.575 activities for analysis, the following information was included for each activity: "Date, time, user code name, terminal name, affected document, and transaction type."

The study used "Artificial Neural Networks" and "Decision Tree" methods, and analyses were carried out with the Matlab program. Before both analyses, the data were categorized as "suspected fraud" and "not suspected fraud" according to some assumptions to make them suitable for the program. The details of this categorization process are given in Table 1.

Table 1: Determination of Fraud Suspect and Non-Fraud Features

Category	Suspected Fraud	No Suspicion of Fraud
In Terms of User Code Definition	Those who do not have a user code definition in the transaction	Those who have a user code definition in the transaction
In terms of hours	Transactions made outside of working hours	Transactions made during working hours
In terms of the number of daily deletions	More than ten deletions in a particular terminal	Deleting ten and down in a particular terminal
In terms of the number of monthly transactions of the user in a particular terminal	Users with 100 and below transactions in a particular terminal	Users with more than 100 monthly transactions on a particular terminal
In terms of the number of daily transactions of the user in a particular terminal	Users with ten or fewer daily transactions on a particular terminal	Users with more than ten daily transactions on a particular terminal

According to Table 1;

- Transactions that do not have a user code are considered "fraud suspects", and those with a user code are "not suspected of fraud",

- Transactions made outside of working hours are considered "fraud suspects", and transactions made during working hours are "not suspected of fraud",

- In terms of the number of deletions per day, those who have more than ten deletions in a particular terminal are "fraud suspects", those with ten or fewer deletions are "not suspected of fraud",

- The number of transactions of a particular user in a particular terminal is 100 or less per month as "fraud suspect", those over 100 as "not suspected of fraud",

- The number of daily transactions of a particular user on a particular terminal is ten or less, “fraud suspect", and more than 10 "fraud suspect".

In the classification made, transactions with suspected fraud are given a value of 1 in the relevant category, and transactions without suspicion of fraud are given a value of 0. Thus, the overall total fraud score was calculated for each transaction. The total fraud score appeared as (0,1,2,3,4). Transactions with 0-2 points, according to the total fraud score, are considered non-fraudulent, and transactions with 3 and 4 fraud points are considered fraudulent.

The consistency of the data used in the created model directly affects the success of the results obtained. For this reason, the data must go through a normalisation process before creating an input to the analysis. Normalization is used in cases with different scales in the total data, which will disrupt the data integrity (Tunç & Ülger, 2016).

The information presented as input to the artificial neural network by normalization is converted to a value between 0 and 1 by the artificial neural network at the input layer. In this conversion, there is only one match for each input value. The formula $x' = \frac{x-x_{min}}{x_{max}-x_{min}}$ is used in this conversion process. This process was carried out by applying separately to all elements with different scales.

Method for neural network analysis

No generally accepted processes exist when creating a model in analyses made with artificial neural networks. The number of neurons whose optimal level is uncertain with certainty constantly changes to obtain optimal results. For this reason, the analysis was performed in the network with the most optimal number of neurons determined by changing the number of neurons in the range of 1-50 in the analysis.

Other features used for training the network;

- Network architecture, “Feed-forward backdrop”,
- Training function, “Levenberg Marquardt (TRAINLM)”,
- Adaptation learning function, “Gradient Descent with Momentum (LEARNGDM)”,
- The performance function, “Mean Squared Error (MSE)”, is used.

During the analysis process, the initial learning of the network took place with 1000 iterations, and the number of neurons with the best results was determined by changing the number of neurons from 1 to 50. In this process, values that gave good results during repeated network learning were encountered in 25, 30, 33 and 35 neuron numbers.

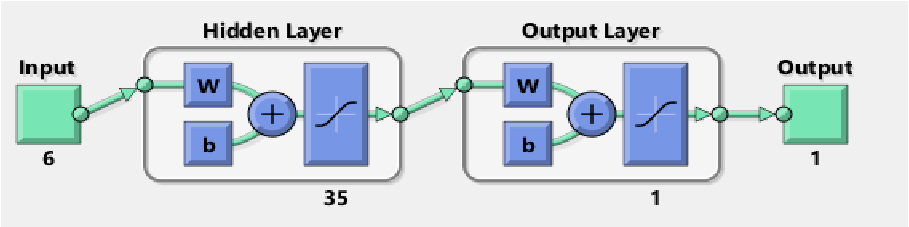


Figure 1: Block Diagram of the Artificial Neural Network Created with the Interface Tool Function

By repeating the learning processes for better learning of the network, the best results were achieved with 35 neurons in 1 iteration value, and an artificial neural network diagram, as in Figure 1, emerged.

Method for decision tree analysis

Before the decision tree analysis, the learning process of the decision tree algorithms was done with all of the "Complex Tree", "Medium Tree", and "Simple Tree" algorithms included in the "Classification Learner" section. When all possibilities are compared, the decision tree analysis was performed with this algorithm since the highest learning rate (100%) was achieved in the "Complex Tree" algorithm.

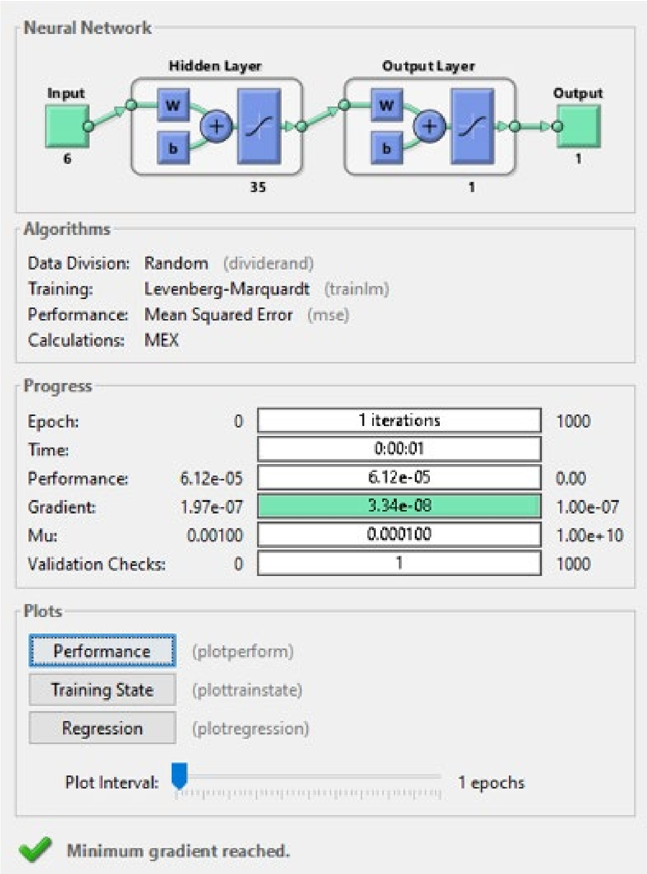
In the analysis process, 502.575 transactions were used, each with six criteria. Decision tree analysis was performed with different learning and testing rates for the program to learn and test it with different data.

Research findings

This section gives the analysis results of artificial neural networks and decision tree methods.

Artificial neural networks analysis results

As seen in Figure 2, in the analysis made with six input data sets, 35 hidden layers, and one output layer, Matlab software randomly selected the learning-validation-test distribution for each learning, and the best learning level was achieved.



Algorithms

Data Division: Random (dividerand)
Training: Levenberg-Marquardt (trainlm)
Performance: Mean Squared Error (mse)
Calculations: MEX

Progress

Epoch:	0	1 iterations	1000
Time:		0:00:01	
Performance:	6.12e-05	6.12e-05	0.00
Gradient:	1.97e-07	3.34e-08	1.00e-07
Mu:	0.00100	0.000100	1.00e+10
Validation Checks:	0	1	1000

Plots

Performance (plotperform)
Training State (plottrainstate)
Regression (plotregression)

Plot Interval: 1 epochs

✓ Minimum gradient reached.

Figure 2: Neural Network Training Interface

The regression values for the network learning realized at the highest level with the repetition of the learning processes according to the number of 35 neurons are shown in Figure 3.

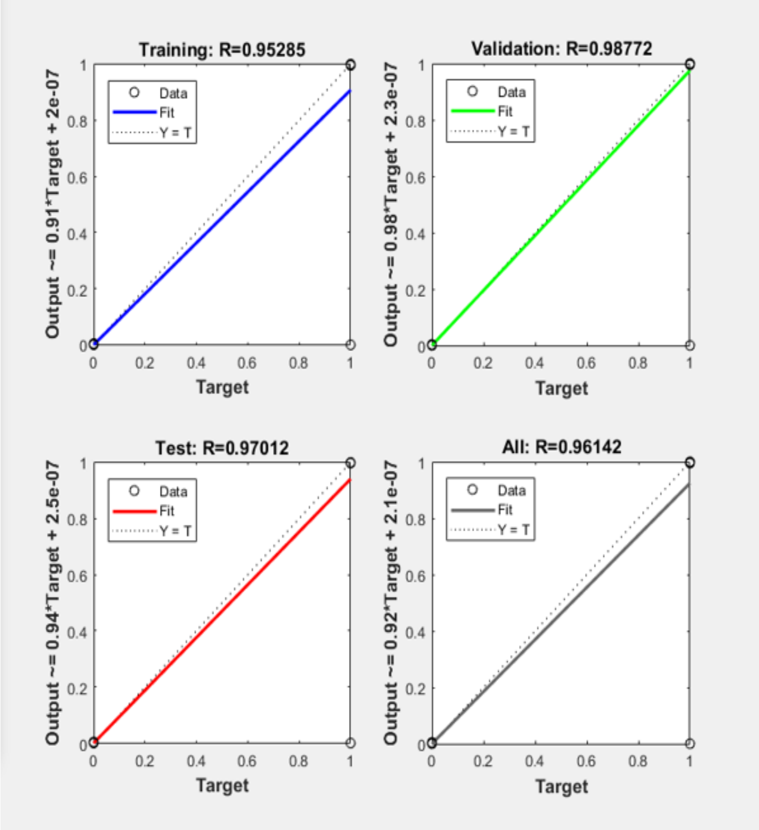


Figure 3: Neural Network Regression Graph

According to Figure 3, RTraining = 0.95285, RValidation = 0.98772, RTest=0.97012 and RAll= 0.96142 were determined as. The fact that these values are close to 1 indicates that the data obtained by the artificial neural network analysis is compatible with the real data (Can & Şencan Şahin, 2021).

A new data set containing 152.575 processes was simulated on the 35-neuron network structure, which was reached as the best value due to training, validating and testing the training within the artificial neural network. The results obtained from the simulation were compared with the actual values of the data in question, and it was concluded that the correct determination was made in 152.268 transactions.

The summary of the elements that are suspected of fraud and those that are not detected as a result of the simulation is shown in Table 2.

Table 2: Summary Table of Success According to Simulation Result

Test	Detected as not suspected of fraud	152.066	69
	Detected as a fraud suspect	238	202
		No Suspicion of Fraud	Suspected Fraud
		Actual Situation	

According to Table 2, the status of 152.066 data was determined correctly among a total of 152.307 data that are not suspected of fraud. A total of 238 data were identified as fraud suspects even though they did not carry any suspicion of fraud. In addition, out of 271 suspected fraudulent data, 202 were detected as fraudulent, and 69 were detected as fraudulent. As a result, it is seen that 152.268/152.575 = 99.7981% correct determination was made.

Decision tree analysis results

The program randomly determined the data sets constituting the learning and testing rates of each model used in this method. The decision tree analysis was performed at four different learning and testing rates, and the findings were included in this section. In addition, the learning-verification-test ratios used in the artificial neural network method took the form of learning testing only due to the data entry alternatives of the program in which the analysis was made in this method.

- **Model 1: Using Data for 90% of Learning and 10% for Testing**

In Model 1, 90% of the data was used for learning and 10% for testing. The details of the data distribution are shown in Table 3.

Table 3: Testing and Learning Rates Between Data (Model 1)

Learning/ Test	**Q**	%
Data Used for Learning	452.318	0.9
Data Used for Testing	50.257	0.1
Total Data	502.575	1

The selection of the data to be used for testing and learning was made randomly by the program, and the analysis result is as in Figure 4.

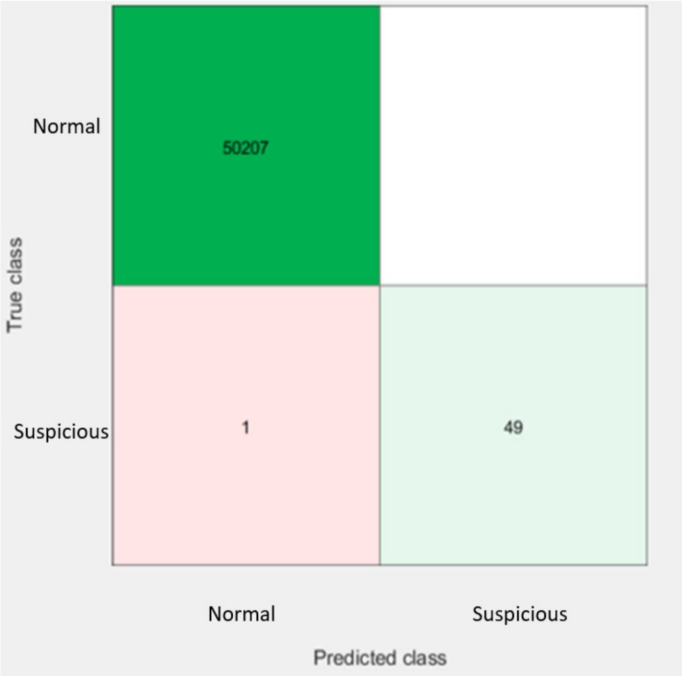


Figure 4: Confusion Matrix (Model 1)

According to Figure 4, when 90% of the data was used for learning, approximately 99.9% was achieved due to the analysis of 10% of the tested part. Only 1 data out of a total of 50.257 data tested was concluded incorrectly.

- **Model 2: Using Data for 85% Learning and 15% for Testing**

In Model 2, 85% of the data was used for learning and 15% for testing. The details of the data distribution are shown in Table 4.

Table 4: Testing and Learning Rates Between Data (Model 2)

Learning/ Test	**Q**	%
Data Used for Learning	427.189	0.85
Data Used for Testing	75.386	0.15
Total Data	502.575	1

The selection of the data to be used for testing and learning was made randomly by the program, and the analysis result is as in Figure 5.

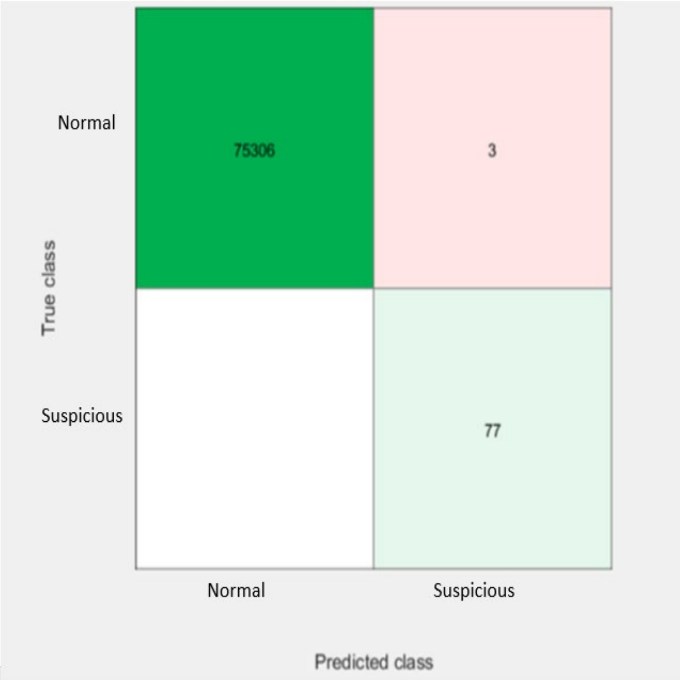


Figure 5: Confusion Matrix (Model 2)

According to Figure 5, when 85% of the data was used for learning, approximately 99.9% was achieved due to the analysis of the 15% test performed. Out of a total of 75.386 data, 3 data were concluded incorrectly.

- **Model 3: Using Data for 75% of Learning and 25% for Testing**

In Model 3, 75% of the data was used for learning and 25% for testing. The details of the data distribution are shown in Table 5.

Table 5: Testing and Learning Rates Between Data (Model 3)

Learning/Test	**Q**	%
Data Used for Learning	376.932	0.75
Data Used for Testing	125.643	0.25
Total Data	502.575	1

The selection of the data to be used for testing and learning was made randomly by the program, and the analysis result is as in Figure 6.

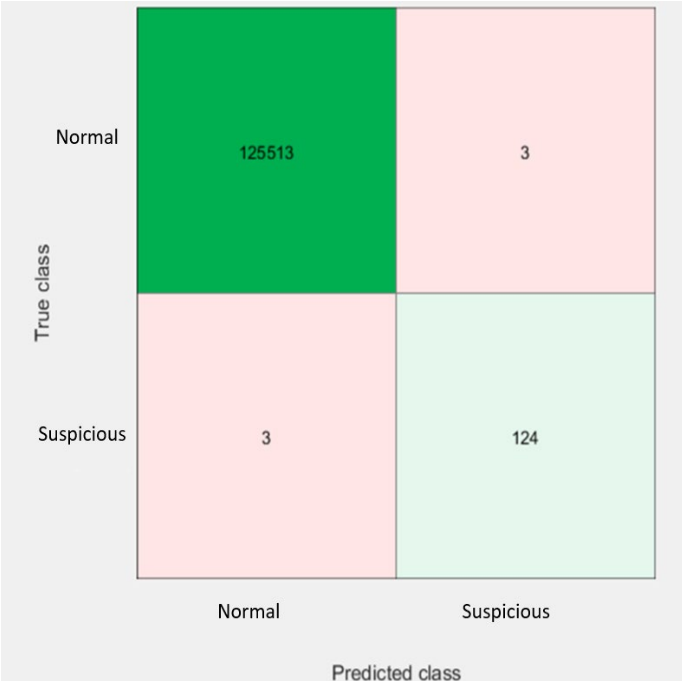


Figure 6: Confusion Matrix (Model 3)

According to Figure 6, when 75% of the data was used for learning, approximately 99.9% was achieved due to the analysis of 25% of the tested part. Six data out of a total of 125.643 data were concluded incorrectly.

- **Model 4: Using Data for 50% Learning and 50% for Testing**

In Model 4, 50% of the data was used for learning and 50% for testing. The details of the data distribution are shown in Table 6.

Table 6: Testing and Learning Rates Between Data (Model 4)

Learning/Test	**Q**	%
Data Used for Learning	251.288	0.5
Data Used for Testing	251.287	0.5
Total Data	502.575	1

The selection of the data to be used for testing and learning was made randomly by the program, and the analysis result is as in Figure 7.

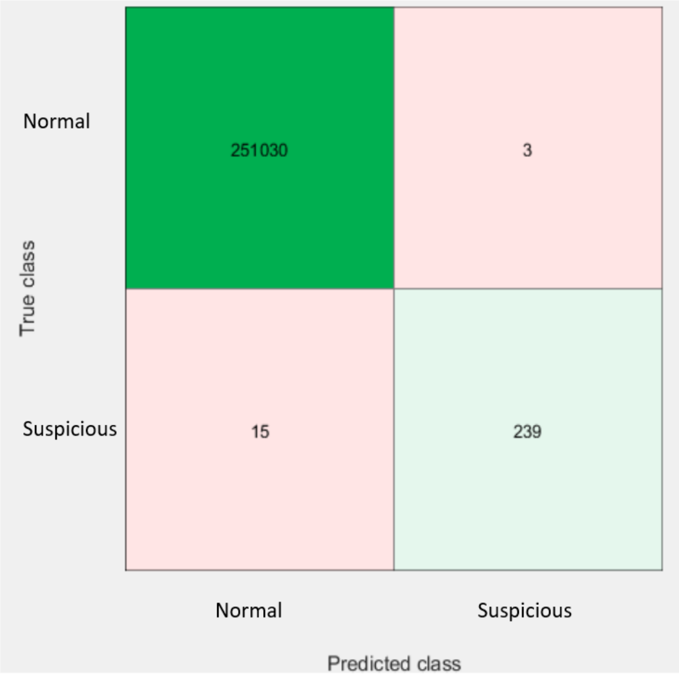


Figure 7: Confusion Matrix (Model 4)

According to Figure 7, when 50% of the data was used for learning, approximately 99.9% was achieved due to the analysis of 50% of the tested part. Eighteen data out of a total of 251.287 data were concluded incorrectly.

Comparison of findings

Successful results have been achieved in both artificial neural networks and decision tree methods. As a result of the analysis made with artificial neural networks, the detection of the risk of fraud or error was 99,7981% accurate. In contrast, the analysis results of the decision tree are shown in Table 7 for each model.

Table 7: Comparison of Decision Tree Models

Models	Number of Correctly Detected Data	Number of Incorrectly Detected Data	Total Data
Model 1 10% Testing, 90% Learning	50.256	1	50.257
Model 2 15% Testing, 85% Learning	75.383	3	75.386
Model 3 25% Testing, 75% Learning	125.637	6	125.643
Model 4 50% Testing, 50% Learning	251.269	18	251.287

According to Table 7, the correct estimation in all models created by changing the ratios used for learning and testing was approximately 99.9899%, close to each other. With the increase in the data used for the test, the number of data the model could not detect, in other words, it detected incorrectly, also increased. The least number of errors were seen in model 1, with the highest learning rate, and the highest number of errors in model 4, with the lowest learning rate.

When the values obtained from artificial neural networks and decision tree analysis methods are compared, it can be said that optimal results are obtained in both methods. However, the decision tree method gave more optimal results with a very low margin of 0.1%. The biggest reason the analysis results give optimal results in both methods is that no sample is created according to any statistical method from the transactions made within six months, and the whole process is included in the analysis. Thus, all transactions represented themselves in the analysis process, and a full count was made.

Conclusion

Data mining has recently gained widespread interest and popularity in different fields worldwide. With data mining applications, the use and efficiency of data mining have increased and become a common trend in many fields. Data mining techniques are increasing in many disciplines, including accounting, which has many business applications. Regarding accounting, data mining is an important technology for the twenty-first century. However, data mining techniques in academic research in accounting are still in their infancy. Accounting has not benefited from sufficient data mining power and capabilities.

This study tests decision trees and artificial neural networks for their applicability in fraud detection. Transactions in the company were analysed in terms of date, time, user code name, terminal name, affected document and transaction type. As a result of the analysis, it has been determined that both methods have very high accuracy rates. Similar results regarding the operation performed with artificial neural network analysis were achieved by Jan (2018) with 90.83%, Terzi and Kıymetli Şen (2015) with 100%, and Gür and Tarhan Mengi (2022) with 99.35% correct detection rates. Similar results regarding the operation performed with decision tree analysis were achieved by Liou (2008) with 100%, Gür and Tarhan Mengi (2022) with 99.42%, and Gür (2023) with 98% correct detection rates. In addition to these results, when the data mining methods used together for fraud detection are compared, Kotsiantis et al. (2006) and Gür and Tarhan Mengi (2022) state that the decision tree is the method that makes fast and accurate detection. This highlighted interpretation is also consistent with the result of this study. In addition to these conclusions, mentioning the study's limitations would be appropriate.

First, the study was limited to the six-month data of a company. Due to the workload of the business, a maximum 6-month data access limit has been introduced for the study. Although the total number of transactions used in the study was 502.575, the study could be expanded by including a wider timeframe and different types of transactions. Thus, a better approach may be to include many transactions. Second, accuracy results could be compared using different data mining methods in addition to artificial neural networks and decision trees for data analysis. The difficulties experienced while conducting the study can be considered suggestions for future studies. Our recommendations for future work are as follows. The first suggestion is to apply data mining methods based on longer-term real data. The second suggestion is to test different models on the same data and to make comparisons between methods.

Peer-review:

Externally peer-reviewed

Conflict of interests:

The authors have no conflict of interest to declare.

Grant Support:

The authors declared that this study has received no financial support.

Author Contributions:

Idea/Concept/Design: **J.S., İ.K., Y.I.** Data Collection and/or Processing: **Y.I., İ.K., J.S.** Analysis and/or Interpretation: **Y.I., İ.K., J.S.** Literature Review: **İ.K., Y.I., J.S.** Writing the Article: **İ.K., Y.I., J.S.** Critical Review: Approval:

References

ACFE (2022). Occupational Fraud 2022: A Report to the nations, https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf

Aksoy, B. (2021). Finansal tablo hileleri'nin makine öğrenmesi yöntemleri ve lojistik regresyon kullanılarak tahmin edilmesi: Borsa İstanbul örneği. Maliye ve Finans Yazıları, (115), 29-60.

Albizri, A., Appelbaum, D., & Rizzotto, N. (2019). Evaluation of financial statements fraud detection research: a multidisciplinary analysis. International Journal of Disclosure and Governance, 16, 206–241.

Amani, F., & Fadlalla, A. (2017). Data mining applications in accounting: A review of the literature and organizing framework. International Journal of Accounting Information Systems, 24, 32-58.

Ata, H., & Seyrek, I. (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.

Baldwin, A., Brown, C., & Trinkle, B. (2006). Opportunities for artificial intelligence development in the accounting domain: the case for auditing. Intelligent Systems in Accounting, Finance and Management, 14(3), 77-86.

Can, N., & Şencan Şahin, A. (2021). Yapay sinir ağları metodu ile günlük çiğ noktası sıcaklığı tahmini. Gümüşhane Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 11(4), 1154-1163.

Dayı, F., & Ata, H.A. (2012). Yapay sinir ağı ile hisse senedi getirisi tahmini: Bir firma uygulaması. 16. Finans Sempozyumu, 181-194.

Debreceny, R., & Gray, G. (2010). Data mining journal entries for fraud detection: An exploratory study. International Journal of Accounting Information Systems, 11(3), 157-181.

Dutta, I., Dutta, S., & Raahemii, B. (2017). Detecting financial restatements using data mining techniques. Expert Systems with Applications, 90, 374-393.

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

Gray, G., & Debreceny, R. (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., & Choi, J. (1997). Assessing the risk of management fraud through neural network technology. Auditing: A Journal of Practice and Theory, 16(1), 14-28.

Gür, Ö. (2023). Karar ağacı destekli hile tespiti ve bir uygulama. Alanya Akademik Bakış, 7(1), 511-528.

Gür, Ö., & Tarhan Mengi, B. (2022). Hile tespitinde makine öğrenmesi yöntemlerinin kullanılması ve model performanslarının değerlendirilmesi. İşletme Araştırmaları Dergisi, 14(4), 3053–3065.

Jan, C. (2018) An effective financial statements fraud detection model for the sustainable development of financial markets: Evidence from Taiwan. Sustainability, 10(513), 1-14.

Kara, S., & Özcan, P. (2020) Muhasebe manipülasyonlarında yapay sinir ağlarının önemi ve bir uygulama. Muhasebe ve Denetime Bakış, 20(60), 155-176.

Kılıç, İ., & Önal, S. (2022). Finansal hilelerin tespit edilmesinde kullanılan veri madenciliği yöntemleri ve Borsa İstanbul'da bir uygulama. Muhasebe ve Denetime Bakış, 22(67), 181-208.

Kılıç, İ., & Önal, S. (2021). Finansal hilelerin yapay sinir ağları yöntemi ile tespit edilmesi. İksad Publishing House, 230 s, Ankara.

Kılıç, Y., & Seyrek, İ. (2012). Finansal başarısızlık tahmininde yapay sinir ağlarının kullanılması: İmalat sektöründe bir uygulama, 1. International Symposium on Accounting and Finance, 1-15.

Kırda, K., & Katkat Özçelik, M. (2021). Finansal tablo hilesi riski taşıyan şirketlerin veri madenciliği ile belirlenmesi. Journal of Accounting and Taxation Studies, 14(2), 609-639.

Kıymetli Şen, İ., & Terzi, S. (2022) Yapay zeka ve dijital muhasebe trendlerinde muhasebe eğitimine ilişkin öneriler. Journal of Business in The Digital Age, 5(2), 105-113.

Kıymetli Şen, İ., & Terzi, S. (2012). Detecting falsified financial statements using data mining: Empirical research on finance sector in Turkey. Maliye Finans Yazıları, 26(96), 76-94.

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.

Kirkos, E., Spathis, C., & Manolopoulos, Y. (2008). Support vector machines, decision trees and neural networks for auditor selection. Journal of Computational Methods in Sciences and Engineering, 8(3), 213-224.

Kopun, D. (2018). A review of the research on data mining techniques in the detection of fraud in financial statements. Journal of Accounting and Management, 8(1), 1-18.

Kotekani, S., & Velchamy, I. (2020). An effective data sampling procedure for imbalanced data learning on health insurance fraud detection. Journal of computing and information technology, 28(4), 269-285.

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.

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

Liou, F.M. (2008). Fraudulent financial reporting detection and business failure prediction models: A comparison. Managerial Auditing Journal, 23(7), 650-662.

Mururorunkwere, B., Tuyishimire, O., Haughton, D., & Nzabanita, J. (2022). Fraud detection using neural networks: A case study of income tax. Future Internet, 14(6), 168.

Ngai, E., Hu, Y., Wong, Y., 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.

Önal, S., & Kılıç, İ. (2019). Hile denetiminde kırmızı bayraklar yöntemi, Çukurova II. Uluslararası Multidisipliner Çalışmalar Kongresi Bildiriler Kitabı, 548-552.

Pérez López, C., Delgado Rodríguez, M., & de Lucas Santos, S. (2019). Tax fraud detection through neural networks: An application using a sample of personal income taxpayers. Future Internet, 11(4), 86.

Rezaee, Z. (2005). Causes, consequences, and deterence of financial statement fraud. Critical Perspectives on Accounting, 16(3), 277-298.

Rukhsar, L., Bangyal, W., Nisar, K., & Nisar, S. (2022). Prediction of insurance fraud detection using machine learning algorithms. Mehran University Research Journal Of Engineering & Technology, 41(1), 33-40.

Seyrek, İ.H., & Ata, H.A. (2010). Veri zarflama analizi ve veri madenciliği ile mevduat bankalarında etkinlik ölçümü. BDDK Bankacılık ve Finansal Piyasalar Dergisi, 4(2), 67-84.

Tang, J., & Karim, K. (2019). Financial fraud detection and big data analytics–implications on auditors' use of fraud brainstorming session. Managerial Auditing Journal, 34(3), 324-337.

Tang, X., Liu, G., Yang, J., & Wei, W. (2018). Knowledge-based financial statement fraud detection system: based on an ontology and a decision tree. Knowledge Organization, 45(3), 205-219.

Tatar, B., & Kıymık, H. (2021). Finansal tablolarda hile riskinin tespit edilmesinde veri madenciliği yöntemlerinin kullanılmasına yönelik bir araştırma. Journal of Yasar University, 16(64), 1700-1719.

Terzi, S. (2012). Hile ve usulsüzlüklerin tespitinde veri madenciliğinin kullanımı. Muhasebe ve Finansman Dergisi, (54), 51-64.

Terzi, S., & Kıymetli Şen, İ. (2015). Adli muhasebede hilelerin tespitinde yapay sinir ağı modelinin kullanımı. International Journal of Economic & Administrative Studies, 7(14), 477-490.

Terzi, S., & Kıymetli Şen, İ. (2012). Finansal tablo hilelerinin veri madenciliği yardımıyla tespit edilmesi: Üretim sektöründe bir araştırma. Journal of Accounting and Taxation Studies, 5(2), 25-40.

Tunç, A., & Ülger, İ. (2016). Veri madenciliği uygulamalarında özellik seçimi için finansal değerlere binning ve five number summary metotları ile normalizasyon işleminin uygulanması, 18. Akademik Bilişim Konferansı, Bildiriler Kitabı, 47-58.

Ugrin, J., & Odom, M. (2010). Exploring Sarbanes–Oxley's effect on attitudes, perceptions of norms, and intentions to commit financial statement fraud from a general deterrence perspective. Journal of Accounting and Public Policy, 29(5), 439-458.

Uğurlu, M., & Sevim, Ş. (2015). A comparative analysis on the relative success of mixed-models for financial statement fraud risk estimation. Gaziantep University Journal of Social Sciences, 14(1), 65-88.

Ulucan Özkul, F., & Pektekin, P. (2009). Muhasebe yolsuzluklarının tespitinde adli muhasebecinin rolü ve veri madenciliği tekniklerinin kullanılması. World of Accounting Science, 11(4), 57-88.

Yang, J. (2006). Data mining techniques for auditing attest function and fraud detection. Journal of Forensic Investigative Accounting, 1(1), 4-10.

Yao, J., Zhang, J., & Wang, L. (2018). A financial statement fraud detection model based on hybrid data mining methods. International Conference on Artificial Intelligence and Big Data (ICAIBD), 57-61.

Ye, H., Xiang, L., & Gan, Y. (2019). Detecting financial statement fraud using random forest with SMOTE. In IOP Conference Series: Materials Science and Engineering, 612(5), 052051, IOP Publishing.

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