Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Research Article

Turk J Elec Eng & Comp Sci
(2019) 27: 3633 – 3647
© TÜBİTAK
doi:10.3906/elk-1902-18

Detection of fraud risks in retailing sector using MLP and SVM techniques

Davut PEHLİVANLI[1], **Süleyman EKEN**[2*], **Ebubekir AYAN**[3]
[1]Department of Business Administration, Faculty of Political Sciences, İstanbul University, İstanbul, Turkey
[2]Department of Computer Engineering, Kocaeli University, Kocaeli, Turkey
[3]Department of Business Administration, Kocaeli University, Kocaeli, Turkey

Received: 03.02.2019 • **Accepted/Published Online:** 15.04.2019 • **Final Version:** 18.09.2019

Abstract: In today's business conditions, where business activities are spreading over a wide geographical area, fraud auditing processes have crucial importance especially for the retailing sector which has a high branch network. In the retailing sector, especially purchasing processes are subject to high fraud risks. This paper shows that it is possible to detect fraudulent processes by applying data mining techniques on operational data related to purchasing activities. Within this scope, in order to detect the fraudulent purchasing operations, support vector machine (SVM) models with different kernels and artificial neural networks methods have been used and successful results have been achieved. The results of the two methods have been examined comparatively and it shows that optimized SVM classifier outperforms others. Besides, in this study, it is presumed that the detected fraud data can be proactively used in the struggle against fraud with fraud-governance risk and compliance software by converting it into scenario analysis.

Key words: Retail sector, risk management, purchase fraud, governance risk and compliance

1. Introduction

The concept of fraud is defined in various forms in the auditing literature. The Association of Certified Fraud Examiners (ACFE) defines fraud as *the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets*. In more general terms, regardless of the type of fraud, fraud is a deliberately deceptive and misleading activity that is different from definitions of normal behavior [1]. In today's business world, having an effective fraud auditing system is a crucial necessity especially for large-scale businesses. Fraudulent transactions can cause enormous damages to businesses and national economies. Branching is increasing rapidly, business activities spread to wide areas and consequently auditing activities become physically more complex, businesses are heavily exposed to the fraud risk and its negative influences more than ever. In this respect, being able to detect fraudulent processes in advance hold great significance in terms of both businesses and the efficiency of the economy.

With the impact of recent developments in information technology, it has become increasingly difficult to identify fraudulent activities among these large transaction volumes, as stored data begins to reach huge dimensions. As a result, auditing processes have become increasingly dependent on technology [2]. Carrying out the purchasing and payment processes in a computer-based environment does not remove or reduce the possibility of fraudulent transactions. On the contrary, traditional auditing processes have been losing their efficiency since the events that appear in concrete form in manual applications are carried on a more abstract environment in computer-based systems [3]. Thus, auditing activities related to purchasing and payment

[*]Correspondence: suleyman.eken@kocaeli.edu.tr

processes should be designed and carried out much more carefully and professionally in today's business world. To avoid incurring losses arising from fraud, a variety of activities have been carried out as fraud prevention, fraud deterrence, and fraud detection [4]. Basically, it is possible to state that the first stage to secure businesses from fraud risks is the prevention of fraudulent activities. Put simply, fraud prevention is the task to stop fraud from happening in the first place. It is implemented by improving technologies and designs. However, this approach is not always successful and is occasionally infiltrated by fraudsters. In that case, fraud detection is the next layer of defense [5].

In previous years, manual fraud audit techniques have been used to detect fraud. These complicated and time-consuming techniques were practiced in various areas. Therefore, to raise the effectiveness of detection, computerized and automated fraud detection systems were developed. However, fraud detection system capabilities were limited because the detection fundamentally depends on predefined rules that are stated by experts. And what is more, the effectiveness of fraud detection methods can turn into another fraud risk. As a consequence, in addition to the fraud triangle (incentives, attitudes, and opportunities), the failure of the auditing procedures has been added to the scope of the fraud risk as a risk factor [6]. Then, more complex fraud detection systems integrating a wide range of data mining methods have been developed for more effective fraud detection [7].

Our study aims to evaluate data containing purchasing budget records, operational purchasing targets and some probable fraudulent purchasing transactions in the retailing sector. In the retailing sector, reaching the purchasing goals and profitability targets are directly and strongly related concepts. Businesses determine their operational targets in accordance with their strategic targets and set their purchasing budgets accordingly. Purchase budget is the primary budget that affects net profitability for the commercial businesses. Some important operational targets of purchasing departments are stock turnover, shelf life, gross income, and optimum inventory cost. Figures of these indicators constitute the basic data for the fraud detection of purchasing processes.

Just like it is in other sectors, purchasing fraud is a critical risk factor in the retailing sector as well. It is highly important to identify purchasing fraud risk, but not sufficient. These risks also have to be managed dynamically in real time. Otherwise, preventing the wrongful and/or fraudulent purchasing activities is not possible in the short term, because the purchasing plans are completed one year prior to the related season.

Examining the previous studies, it is seen that generally financial statement frauds have been assessed, using the published financial statements data. Frauds based on business operations are harder to detect compared to financial statement frauds. These operational frauds have rarely been taken as subjects for academic studies due to the low possibility of these identified fraudulent processes to be shared with third parties.

The auditors use analytical techniques to detect fraudulent transactions [8, 9]. By using data mining techniques, any kind of fraud risk that may be experienced in the procurement process can be defined. Afterward, with the scenario analyses located in the fraud and/or governance risk and compliance (GRC) software, streaming data of the business can be monitored in terms of fraud risk in real time, so precautions against the frauds can be implemented accordingly. The transactions that are confirmed to be fraudulent by data mining techniques required to be built on dynamic business data through scenario-based software. On the condition that these scenarios are located successfully, business data will be instantly evaluated in terms of fraud risk, and thus a systematic study to prevent fraud will be started.

Moving along with operational data of the businesses, this study aims to reveal that it is possible to manage proactively the frauds arising from the purchase, production, selling, human resources, finance, and accounting departments, and data mining techniques can provide a significant infrastructure in that process. Managers operating in intense data environment can define and evaluate their risks, compose their policies and rules, and prepare scenarios, according to the model in such studies. With this infrastructure, when scenario-based software is applied, businesses can proactively conduct risk management processes effectively with the real-time data to be received from ERP databases. Main contributions of this paper are:

- We build a new public fraud dataset.
- Support vector machine (SVM)- and a multilayer perceptron (MLP)-based solutions are proposed to classify if attributes in a transaction record are fraudulent or nonfraudulent. Based on the results, it proposes a risk scenario which can be used in a scenario-based fraud-risk software.

The next parts of this paper are organized as follows: After the literature review, in Section 3, fraud and risk management concepts are generally evaluated, and the subjects of integrating scenario analyses with the data mining techniques are analyzed. In Section 4, the methodology of our research and analysis results are explained. In Section 5, how dynamic scenario analysis can be applied to the business database is evaluated. The last section concludes the article.

2. Related works

The studies concerning the detection of financial statement fraud generally show that data mining techniques increase the probability of fraud detection. In these studies, generally, the relation between fraudulent financial statement data and red flags or the relations between financial statement frauds and a specific risk factor have been analyzed. The main ones of these studies are on credit card frauds, credit default risk, and stock price manipulation [10–17]. Some selected studies in accordance with the goal of our study will be briefly discussed below.

Yeh and Lien [18] and Sanchez et al. [13] focus on the detection of operational fraud. They studied operational data analysis and detection of purchase frauds. According to Sanchez's work, thanks to the instantly monitored systems of business operational data, operational risks can be reduced and thus, profitability can be increased. Our study shows similarity with the main ideas of this study and focuses on the assumption that the frauds detected by data mining techniques can be detected on the simultaneous scenario-based data. Diaz et al. [19] emphasized that the possibility of detecting share price manipulations through traditional methods is limited. By using data related to liquidity and volatility reflecting probable share price operations, the authors have been able to form more qualitative relation analyses between data mining techniques and price manipulation. In the study, relation patterns that can be used in detecting fraud are reported as decision trees. The results show the significance of monitoring changes in transaction volume and volatility for determining the price manipulations. Didimo et al. [20] state that data mining techniques and software can be used in order to detect financial crimes and fraud schemes that may arise in the banking or insurance sectors. Particularly in the conclusion part of the study, it is advised to focus on the dynamic application of methods such as networks by combining multiscale force-directed algorithms with geometric constraints, which can be used in the future for identifying financial crimes and schemes.

Uğurlu and Sevim [21] studied the management of frauds that may cause credit risk in the banking sector. Because of the high importance of financial statement accuracy and reliability in the banking sector for credit risk management, they tried to make it possible to predict fraud risk that could be committed in financial statements. They utilized the artificial neural networks (ANN) methodology using financial data of 289 firms, and their model reached successful results in predicting financial statement frauds with an accuracy of 90%. Omar et al. [22] focused on the prediction of financial reporting frauds, using ANN. They aimed to explore the effectiveness of ANN in predicting fraudulent financial reporting for small market capitalization companies in Malaysia. They applied their mathematical model among selected fraud and nonfraud companies comparatively. Ten separate financial ratios were used as fraud risk indicators to predict fraudulent financial reporting using ANN. Their findings indicate that the proposed ANN methodology outperforms other statistical techniques widely used for predicting fraudulent financial reporting.

Lin et al. [23] investigated the differences between data mining techniques and experts' judgments. They used expert questionnaires and data mining techniques including logistic regression, classification and decision trees (CART), and ANN. According to their findings, the ANN and CART approaches work with the training and testing samples in a correct classification rate of 91.2% (ANN) & 90.4% (CART) and 92.8% (ANN) & 90.3% (CART), respectively, which is more accurate than the logistic model that only reaches 83.7% and 88.5% of the correct classification in assessing the fraud presence. They also indicated that from the top ten critical fraud factors in different prediction models, judgments of experts are most consistent with the CART prediction model.

3. Fraud and risk management

Fraud is an unfair gain obtained by personnel, using or acquiring the resources and assets of the company in an intentionally improper way. Possible frauds in the retailing sector can be sorted as purchase frauds, cash-safe frauds, customer and employee thief frauds, sales frauds, discount frauds, return frauds, and overtime frauds. According to the global fraud report regularly issued by ACFE; the proportional distribution of retailing sector frauds consist of 32.7% corruption, 32.7% noncash, 17.3% skimming, 15.4% billing, 12.5% cash larceny, 11.5% cash on hand, 9.6% check tampering, 8.7% expense reimbursements, 8.7% register disbursements, 5.8% financial statement fraud 3.8% are payroll frauds.

It is possible to manage the frauds other than purchasing frauds mostly right after they are detected by antifraud measures. However, purchase frauds are very hard to manage in the current period in the retailing sector, and usually, the determined antifraud actions can be applied within the next purchasing period. Realized purchase frauds can be proactively inferred from key performance indicators, such as declining gross profit margins, prolonged stock shelf life, and a tendency for stock turnover rates to fall. In the retailing sector, purchasing decisions are mostly determined one year in advance and orders are given accordingly. Therefore, even if these kinds of frauds are detected, the possibility of imposing a sanction and compensating the loss of the business within the current year is rather low.

In terms of auditing, detection of fraudulent transactions is not an easy action. Especially, detection of the fraudulent activities involving the executive levels in the fraud scheme is even more difficult. The most important shortcomings of the auditing processes against fraudulent transactions are management's concealing fraudulent transactions, inadequate information about management processes, inadequate experience on the fraudulent transaction and misleading of the auditors [24].

From a risk management perspective, fraudulent attempts can be proactively managed in scenario-based fraud and GRC software. But in fraud and/or GRC type software, detection of the predicted fraud attempt processes are performed by using defined relation analyses. Thus, it is naturally impossible to detect and monitor fraud attempts that have not yet been identified and that have not been the subject of contradiction. Therefore, firstly, business data should be analyzed in detailed with data mining techniques, then required scenarios should be created for all kinds of detected risks and frauds, and subsequent processes should be managed by the help of fraud and/or GRC software.

As shown Figure 1, in this context, scenarios are built with the data produced by the data mining techniques, then tested and make some detail adjustments, and finally, the scenarios run in real time in the fraud and/or GRC software. In this process, the outputs of the risk management activities should be integrated into the risk assessment process, especially during the planning phase of the auditing. The greatest benefit of using risk management outputs in the auditing phase is the partial elimination of audit risks that may be faced with human error or other reasons.

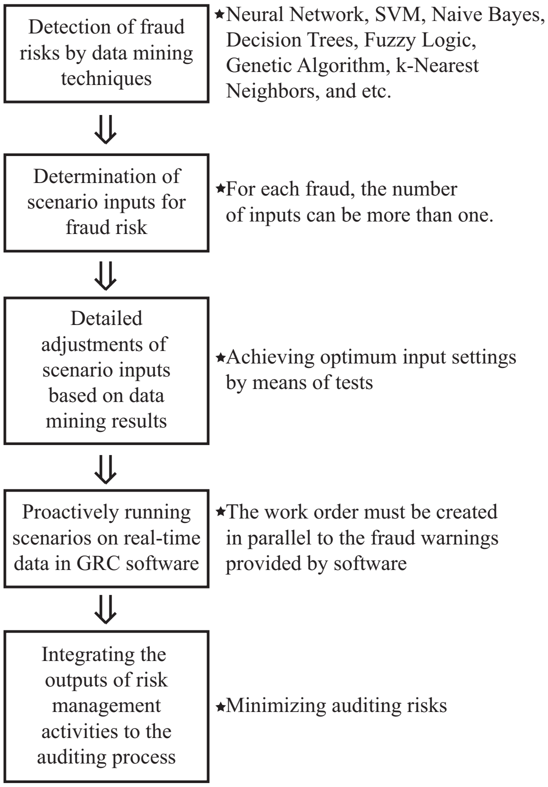
Detection of fraud risks by data mining techniques
★Neural Network, SVM, Naive Bayes, Decision Trees, Fuzzy Logic, Genetic Algorithm, k-Nearest Neighbors, and etc.
Determination of scenario inputs for fraud risk
★For each fraud, the number of inputs can be more than one.
Detailed adjustments of scenario inputs based on data mining results
★Achieving optimum input settings by means of tests
Proactively running scenarios on real-time data in GRC software
★The work order must be created in parallel to the fraud warnings provided by software
Integrating the outputs of risk management activities to the auditing process
★Minimizing auditing risks

Figure 1. From data mining to risk management methodology and audit methodology.

4. Methodology and experimental results

As illustrated in Figure 2, a typical fraud detection workflow has the following steps:

- Feature engineering to transform historical data into feature and label inputs for a machine learning algorithm.
- Split the data into two parts, one for building the model and one for testing the model.
- Build the model with the training features and labels.
- Test the model with the test features to get predictions. Compare the test predictions to the test labels.
- Loop until satisfied with the model accuracy:

– Adjust the model fitting parameters, and repeat tests.

– Adjust the features and/or machine learning algorithm and repeat tests.

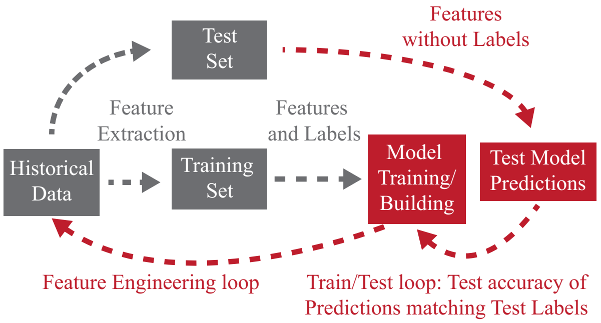

Figure 2. Model building workflow.

Implementation of appropriate approaches, to identify fraudulent activities in financial transactions and to minimize the effects of these crimes by audit firms, contributes to the determination of financial crime. Data mining methods are used effectively in the process of identifying voluntary or involuntary frauds in financial statements and correlation between data. Data mining used to detect financial crimes has many other scientific application areas such as fraudulent purchases, retail industry, telecommunication industry, biological data analysis, classification and analysis of customers. According to the classification of Han et al. [25], models used in data mining are examined under four main topics as classification, clustering, association rules, and time series. Esen [26] specified that data mining approaches used in banking, insurance, securities crimes, and other crimes are categorized as clustering, outlier detection, estimation, regression analysis, and visualization. In this study, ANNs and SVMs were used in the detection of fraudulent purchases. Financial transaction classification is the categorization of the transactions based on predefined classes or types. Here we have two different predefined classes, and we want to classify each transaction according to the two classes. These classes are fraudulent and nonfraudulent data. In the following subsections, these methods are explained in detail.

4.1. Support vector machine

SVM is an effective machine learning method that operates according to the principle of minimizing structural risk in the classification of linear and nonlinear data. It comprises supervised learning methods used for classification, regression, and outlier detection [27]. Classification problem is a binary classification in this paper.

Given training samples (x_i, y_i) for i=1...N, with $x_i \in R^d$ and $y_i \in -1, +1$
SVM algorithm is based on finding the hyperplane that gives the largest minimum distance to the training examples. By considering training data, each disjunctive hyperplane must prepare two conditions given in Eq. (1) for two classes:

$$f(x_i) = \begin{cases} \geq +1, & y_i = +1 \\ \leq -1, & y_i = -1 \end{cases} . \tag{1}$$

For a correct classification, $y_i f(x_i)$ is greater than zero. A linear classifier $f(x_i)$ has the form as shown in Eq. (2):

$$f(x_i) = w^T x_i + b \tag{2}$$

Here w is normal to the line, and b the bias. w is known as the weight vector. The training data is used to learn w. The positive and negative support vectors are shown in Eq. (3), respectively:

$$\begin{array}{l} w^T x_+ + b = +1 \\ w^T x_- + b = -1 \end{array}, \tag{3}$$

Then the margin is given by Eq. (4):

$$\frac{w}{||w||}(x_+ - x_-) = \frac{w^T(x_+ - x_-)}{||w||} = \frac{2}{||w||}. \tag{4}$$

Learning the SVM can be formulated as an optimization as shown in Eq. (5). This is an optimization problem subject to linear constraints.

$$\begin{array}{ll} \max\limits_{w} & \frac{2}{||w||} \\ \text{s.t.} & y_i(w^T x_i) - b = 1,\ i = 1, \ldots, N \end{array} \tag{5}$$

4.2. Multilayer perceptron

There are thousands of types of specific neural networks proposed by researchers as modifications or tweaks to existing models for different purposes [28, 29], and sometimes as wholly new approaches. A multilayer perceptron is a class of feedforward neural network. It is composed of more than one perceptron. They are composed of an input layer to receive the signal, an output layer that makes a decision or prediction about the input, and in between those two, an arbitrary number of hidden layers that are the true computational engine of the MLP. MLPs with one hidden layer are capable of approximating any continuous function.

MLPs are often applied to supervised learning problems: they train on a set of input-output pairs and learn to model the correlation (or dependencies) between those inputs and outputs. Training involves adjusting the parameters, or the weights and biases, of the model in order to minimize error. Backpropagation is used to make those weigh and bias adjustments relative to the error, and the error itself can be measured in a variety of ways.

4.3. Building dataset

In this paper, we collect our own fraud dataset. It is the monthly operational data belonging to the years 2009–2014 of a shopping center with multiple departmental structures in Turkey. The dataset consists of 1131 samples, each sample has eight attributes: “Purchase Amount”, “Sales Amount”, “Cost of Sales”, “Sales Profit”, “Profit”, “Stock Amount (Quantity)”, “Stock Amount (Value)”, and “Stock Turnover”. The samples are classified using two classes ’fraudulent’ and ’nonfraudulent’ (see Table 1). In fraud detection applications, it is common to encounter datasets showing very high-class imbalance (most often a vast majority of samples belongs to the ’nonfraudulent’ class). Here the percentage of samples that belongs to ’nonfraudulent’ class is 78%. However, most machine learning algorithms do not work very well with imbalanced datasets. Thus, upsampling minority class approach is used to tackle the imbalance problem. Upsampling is the process of randomly duplicating observations from the minority class in order to reinforce its signal. In this study, 70% of the data (791 samples) were reserved for training, 30% (340 samples) for testing.

The results obtained with the help of data mining techniques demonstrate the risks of fraud that businesses may be exposed during the purchasing process within certain possibilities. Basically, in this study, it was tested that the indicators below could be used to reveal purchase-originated frauds.

Red flags are selected from key performance indicators for purchasing operations and which can be used to identify fraudulent transactions are listed below:

A: Low gross profitability on product and supplier basis

B: Low stock turnover ratio on product and supplier basis

C: High stock cost on product and supplier basis

D: High shelf life on product and supplier basis

Table 1. Attributes of retail fraud dataset.

Attributes of retail fraud dataset	Explanation
Purchase amount	0 – 170.000 USD
Sales amount	0 – 279.000 USD
Cost of sales	0 – 172.000 USD
Sales profit	~116.000 USD
Profit	20%(Avg)
Stock amount (quantity)	0 – 12.967
Stock amount (value)	0 – 188.000 USD
Stock turnover	9.5 (Avg)

Moreover, it is always a good idea to look into correlation coefficients between each variable and the others. Figure 3 shows the heat map for correlation matrix. Colors indicate strength of the linear relationships between data. For example, the linear relationship strength increases as the color opens.

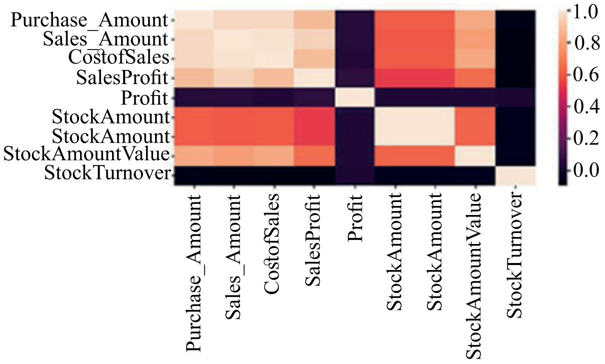

Figure 3. Correlations between attributes of retail fraud dataset.

4.4. Performance results and analysis of classification methods

The confusion matrix is used to describe the performance of classification algorithms by calculating performance metrics. In this study, for measuring the performance of the methods used, the following metrics have been used:

- True Positive (TP) - Indicates positive instances correctly classified as positive outputs
- True Negative (TN) - Indicates negative instances correctly classified as negative outputs
- False Positive (FP) - Indicates negative instances wrongly classified as positive outputs
- False Negative (FN) - Indicates positive instances wrongly classified as negative output
- Classification Precision (PR) - Indicates the number of true positives over the number of true positives plus the number of false positives
- Classification Recall (CR) - Indicates the the number of true positives over the number of true positives plus the number of false negatives
- F_1-score - Indicates the the harmonic mean of precision and recall

In our experiments, we use a machine which has a single core Intel Core i7-950 3.0 GHz processor, 8GB DRAM memory, and 1TB SATA2 7200RPM hard disk. The operating system Ubuntu Linux 10.10 is installed on the machine. The main data mining techniques, ANNs and SVM methods have been implemented in Python environment. Scikit-learn module is used to integrate these machine learning algorithms. All samples in the dataset are divided into two categories (fraudulent and nonfraudulent transactions) by means of supervisor. For each category, randomly selected samples are used for training and other samples are used as a test sample. This allows generalization of real, previously unseen data. Instead of having a single train/test split, we specify so-called folds so that the data is divided into similarly-sized folds. Training occurs by taking all folds except one—referred to as the holdout sample. On the completion of the training, the performance of the fitted model is tested using the holdout sample. The holdout sample is then thrown back with the rest of the other folds, and a different fold is pulled out as the new holdout sample. Training is repeated again with the remaining folds and we measure performance using the holdout sample. This process is repeated until each fold has had a chance to be a test or holdout sample. Here, 10-fold cross-validation is used. Figure 4 shows the confusion matrix for SVM classifier (0 for nonfraudulent, 1 for fraudulent). Table 2 presents performance metrics for SVM classifier on retail fraud dataset.

Table 2. Performance metrics for SVM classifier on retail fraud dataset.

Classes	Precision	Recall	F_1-score	Support
Nonfraudulent	0.89	1.00	0.94	267
Fraudulent	1.00	0.55	0.71	73
Avg/Total	0.91	0.90	0.89	340

Machine learning models are parameterized so that their behavior can be tuned for a given problem. Models can have many parameters and finding the best combination of parameters can be treated as a search problem. In this paper, we aim to tune parameters of the SVM classification model using scikit-learn. Two

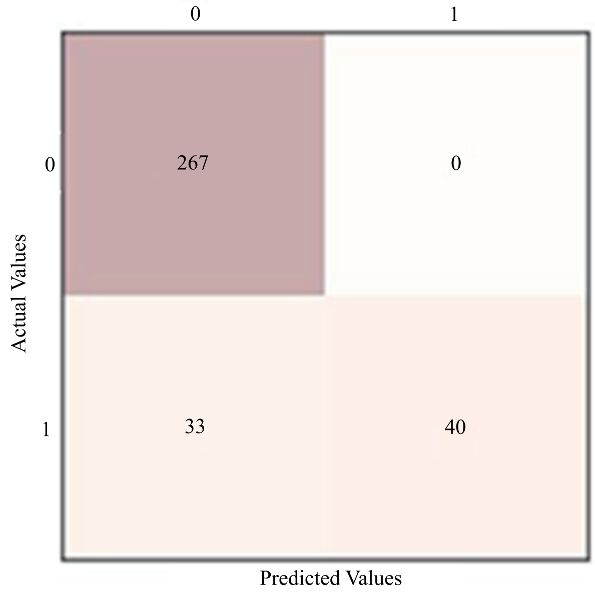

Figure 4. Confusion matrices of SVM classifier on retail fraud dataset.

key parameters of the SVM algorithm can be tuned: the value of C (how much to relax the margin) and the type of kernel. The default for SVM (the SVC class) is to use the radial basis function (RBF) kernel [30] with a C value set to 1.0. We perform a grid search using 10-fold cross validation with a standardized copy of the training dataset. We try a number of simpler kernel types as shown in Eq. (6) (linear, polynomial, RBF, and sigmoid) and C values with less bias and more bias (less than and more than 1.0 respectively). Python scikit-learn provides two simple methods for algorithm parameter tuning: (i) grid search parameter tuning and (ii) random search parameter tuning. After SVM parameter optimization, the best parameters are 'C': 100.0, 'kernel': 'linear', 'gamma': 0.001 obtained. Figure 5 shows the confusion matrix for SVM parameter tuning. Table 3 presents performance metrics. Figure 6 illustrates the decision boundaries produced by the linear, Gaussian, and polynomial classifiers.

$$K(X_i,X_j)=\begin{cases} X_i \bullet X_j, & linear \\ (\gamma X_i \bullet X_j + C)^d, & polynomial \\ exp(-\gamma|X_i - X_j|^2), & RBF \\ tanh(\gamma X_i \bullet X_j + C), & sigmoid \end{cases}, \tag{6}$$

where $K(X_i,X_j)=\phi(X_i)\bullet\phi(X_j)$ that is, the kernel function, represents a dot product of input data points mapped into the higher dimensional feature space by transformation ϕ.

Table 3. Performance metrics for optimized SVM classifier on dataset.

Classes	Precision	Recall	F_1-score	Support
Nonfraudulent	0.97	1.00	0.98	267
Fraudulent	0.98	0.88	0.93	73
Avg/Total	0.97	0.97	0.97	340

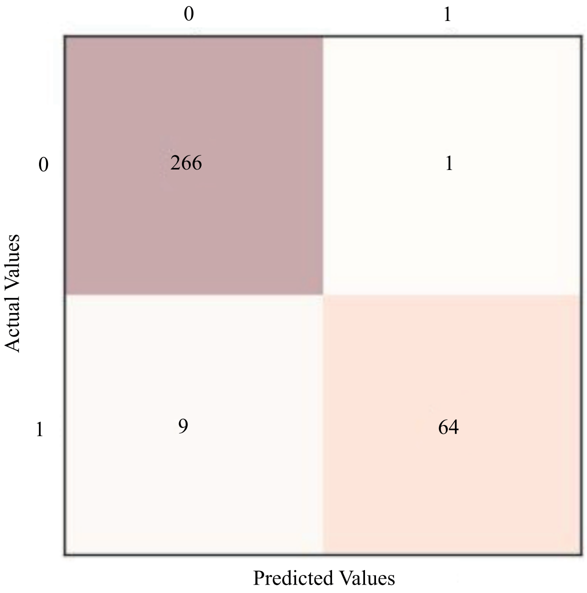

Figure 5. Confusion matrices of optimized SVM classifier on retail fraud dataset.

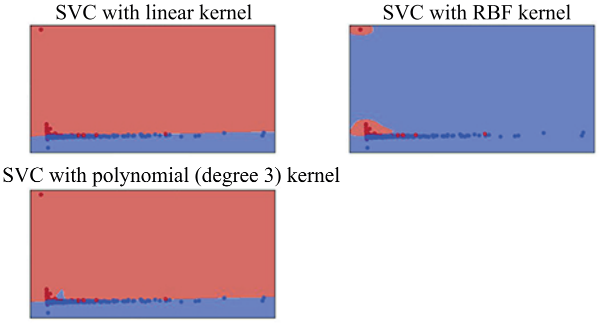

Figure 6. Decision boundaries for different kernel types.

MLP is a supervised learning algorithm that learns a function $f(.) : R^m \rightarrow R^o$ by training on a dataset, where m is the number of dimensions for input and o is the number of dimensions for output. MLP can learn a nonlinear function approximator for classification [31]. In this paper, we implement an MLP algorithm (activation='logistic', alpha=0.0001, batch_size='auto', epsilon=1e-08, hidden_layer_sizes=(40, 40, 40), learning_rate='constant') that trains using backpropagation. Adam [32] is an adaptive learning rate optimization algorithm that has been designed specifically for training neural networks. Here, Adam optimizer is used. MLP is an example of ANN. Here, the number of input layer is eight and the number of output layer is two. Figure 7 shows the confusion matrix for MLP. Table 4 presents performance metrics. When all classifiers are compared, optimized SVM classification with linear kernel outperforms the others.

Table 4. Performance metrics for MLP classifier on retail fraud dataset.

Classes	Precision	Recall	F_1-score	Support
Nonfraudulent	0.96	0.99	0.98	267
Fraudulent	0.97	0.86	0.91	73
Avg/Total	0.96	0.96	0.96	340

Businesses that may be exposed to fraud have been defined in parallel with the risk management and fraud auditing methodologies. In this way, the activities of internal auditing, risk management, and compliance teams in businesses can be carried out in a proactive manner and operated more effectively based on the defined data.

5. Current business applications

The most critical phase of risk management is the detection of risks. Management of undetectable ones and those that are not included in the risk universe are naturally impossible. Data mining techniques can be used to

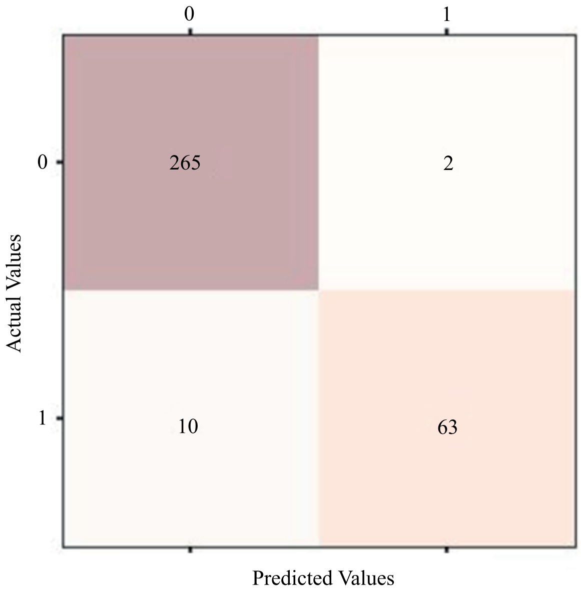

Figure 7. Confusion matrices of MLP classifier on retail fraud dataset.

identify the risks of retailing businesses. In this study, various risks have been identified using SVM and ANN methods. Detection of risks is the first step in fraud risk management process. In the implementation phase, it is necessary to assess the identified risks instantaneously in real-time data and to take risk management actions simultaneously. Otherwise the costs of losses will increase and in other words, risky activities will continue.

In this context, a risk management scenario based on three predetermined risk factors and an exemplary scenario that can be used in GRC or fraud software were created below. Similar scenarios can be created based on risk factors verified in conjunction with data mining results as tabulated in Table 5.

Table 5. Retail sector purchasing fraud risk scenario.

No	Factor	Weight	Scoring
1	Suppliers with gross profitability less than 15%	40	
	Between %10 and %15		5
	Between %0 and %10		10
	%0 and below		25
2	Suppliers with stock turnover ratio 4 and over	40	
	4 and over		7
	Between 3 and 4		10
	Between 0 and 3		23
3	Relationship between low stock turnover and usage of purchasing budget	20	
	Low stock turnover ratio and budget usage more than 100,000 TL		10
	Low stock turnover ratio and budget usage between 50,000 and 100,000 TL		7
	Low stock turnover ratio and budget usage less than 50,000 TL		3

Critical risks can be detected through data mining techniques. The audit manager needs to weight the identified risky activities, test the scenarios created in parallel with business policies and implement them. The scenario inputs and the weighing of those inputs were arranged in accordance with analysis results by SVM and ANN. At this stage, it is necessary to make some fine adjustments in the scoring of the scenarios. During the test phase, input data is increased or decreased to try to reach the most optimal scenario components. At this point, the results obtained by data mining techniques can be used to weight the scenario analysis inputs.

The scenario-based software makes the relevant calculations in conjunction with the working of the exemplary scenario above, during each goods receiving process or after each purchasing operation. Accordingly, operations with a score close to 100 show high tendency to reveal fraudulent transaction and these must be audited immediately.

6. Conclusion

In addition to planning activities of the businesses that operate in a very intense data environment, it is also very important to take some preventive measures within the scope of risk management actions. Preemptive actions in the present day are only more successful compared to manual applications if they are based on systematical and automatic controls.

Auditors are faced with all kinds of frauds that can come from inside and outside of the business, especially management frauds. While the International Internal Auditing Standards do not impose any responsibilities on internal auditors, the expectations from internal auditors are different from those on the current practices.

In this study, purchasing frauds have been detected using SVM and ANN techniques. This study shows that data mining techniques which can be used in the detection of operational frauds, results acquired by data mining techniques can be used as scenario-based through fraud-GRC software and eventually, mentioned probable fraudulent transactions can be taken under the scope of the audit. Scenario-based programs allow suspicious transactions to be monitored simultaneously on the current dynamic business data, so it becomes possible to detect fraudulent activities more effectively.

Proactive management of the purchasing frauds not only helps businesses to achieve their goals but it also prevents frauds that can create financial losses in significant amounts. In this respect, this study can be regarded as a model for preventing frauds that are based on business operations. In this study, it is concluded that the findings achieved through data mining techniques can be used especially in scenario analysis. Accordingly, it is expected that especially the new studies for the detection of fraud through operational data, developing scenarios against the detected fraud types, and application of these scenarios on real-time data will provide significant contributions to the literature. Also in future studies, it should be integrated on the artificial intelligence infrastructure with the outputs of the scenario and the decision processes left to man should be carried out based on artificial intelligence through fully learning algorithms. In this way, an infrastructure is formed in the test of the success percentages of the decision making process of artificial intelligence studies which are introduced into our lives.

References

[1] Zandian ZK, Keyvanpour M. Systematic identification and analysis of different fraud detection approaches based on the strategy ahead. International Journal of Knowledge-Based and Intelligent Engineering Systems 2017; 21: 123-134.

[2] Ertikin K. Hile Denetimi: Kırmızı Bayrakların Tespiti için Kullanılan Proaktif Yaklaşımlar. Muhasebe ve Finansman Dergisi 2017; 75: 71-94 (article in Turkish).

[3] Engin A. İşletmelerde Satın Alma ve Ödeme Süreçlerine Özgü Hile Riskleri ve Uygun İç Kontrol Ortamının Oluşturulması. Mali Çözüm Dergisi 2015; 101-120 (article in Turkish).

[4] Petrucelli JR. Detecting Fraud in Organizations: Techniques, Tools, and Resources. Hoboken, NJ, OSA: John Wiley & Sons, 2013.

[5] Behdad M, Barone L, Bennamoun M, French T. Nature-inspired techniques in the context of fraud detection. IEEE Transactions on Systems, Man, and Cybernetics, Part C 2012; 42(6): 1273-1290.

[6] Srivastava RP, Mock TJ, Lei G. The Dempster-Shafer theory: an introduction and fraud risk assessment illustration. Australian Accounting Review 2011; 21(3): 282-291.

[7] Abdallah A, Maarof MA, Zainal A. Fraud detection system: A survey. Journal of Network and Computer Applications 2016; 68: 90-113.

[8] Kirkos E, Spathis C, Manolopoulos Y. Data Mining techniques for the detection of fraudulent financial statements. Expert Systems with Application 2007; 32(4): 995-1003.

[9] Spathis C, Doumpos M, Zopounidis C. Detecting falsified financial statements: a comparative study using multicriteria analysis and multivariate statistical techniques. European Accounting Review 2002; 11(3): 509-535.

[10] Chen MY. Predicting corporate financial distress based on integration of decision tree classification and logistic regression. Expert Systems with Applications 2011; 38(9): 11261-11272.

[11] Krambia-Kapardis M, Christodoulou C, Agathocleous M. Neural networks: the panacea in fraud detection?. Managerial Auditing Journal 2010; 25: 659-678.

[12] Ravisankar P, Ravi V, Raghava Rao G, Bose I. Detection of financial statement fraud and feature selection using data mining techniques. Decision Support Systems 2011; 50(2): 491-500.

[13] Sánchez D, Vila MA, Cerda L, Serrano JM. Association rules applied to credit card fraud detection. Expert Systems with Applications 2009; 36(2): 3630-3640.

[14] Summers SL, Sweeney JT. Fraudulently misstated financial statements and insider trading: an empiricial analysis. The Accounting Review 1998; 73: 131-146.

[15] Zhou W, Kapoor G. Detecting evolutionary financial statement fraud. Decision Support Systems 2011; 50(3): 570-575.

[16] Ngai EWT, Hu Y, Wong YH, Chen Y, Sun X. The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems 2011; 50(3): 559-569.

[17] Fiore U, De Santis A, Perla F, Zanetti P, Palmieri F. Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. Information Sciences 2017; doi: 10.1016/j.ins.2017.12.030.

[18] Yeh IC, Lien C. The comparisons of data mining techniques for the predictive accuracy of probability of default of credit card clients. Expert Systems with Applications 2009; 36(2): 2473-2480.

[19] Diaz D, Theodoulidis B, Sampaio P. Analysis of stock market manipulations using knowledge discovery techniques applied to intraday trade prices. Expert Systems with Applications 2011; 38(10): 12757-12771.

[20] Didimo W, Liotta G, Montecchiani F. Network visualization for financial crime detection. Journal of Visual Languages & Computing 2014; 25(4): 433-451.

[21] Uğurlu M, Sevim Ş. Artificial neural network methodology in fraud risk prediction on financial statements; an emprical study in banking sector. Journal of Business Research-Turk 2015; 7(1): 60-89.

[22] Omar N, Johari ZA, Smith M. Predicting fraudulent financial reporting using artificial neural network. Journal of Financial Crime 2017; 24(2): 362-387.

[23] Lin CC, Chiu AA, Huang SY, Yen DC. Detecting the financial statement fraud: The analysis of the differences between data mining techniques and experts' judgments. Knowledge-Based Systems 2015; 89: 459-470.

[24] Fanning KM, Cogger KO. Neural network detection of management fraud using published financial data. Intelligent Systems in Accounting, Finance & Management 1998; 7(1): 21-41.

[25] Han J, Kamber J, Pei P. Data Mining: Concepts and Techniques. Burlington, USA: Morgan Kaufmann, 2011.

[26] Esen MF. Finansal suçların tespitinde veri madenciliği yaklaşımı ve literatüre bakış. Eskişehir Osmangazi Üniversitesi İİBF Dergisi 2016; 93-118.

[27] Alpaydın E. Introduction to Machine Learning. Cambridge, MA, USA: MIT Press, 2014.

[28] Yaşar H, Ceylan M. A novel approach for reduction of breast tissue density effects on normal and abnormal masses classification. Journal of Medical Imaging and Health Informatics 2016; 6:3 710-717.

[29] Yaşar H, Serhatlıoğlu S, Kutbay U, Hardalaç F. A novel approach for estimation of coronary artery calcium score class using ANN and body mass index, age and gender data. In: 2018 International Conference on Computer and Technology Applications; Istanbul, Turkey; 2018. pp. 184-187.

[30] Cristianini N, Shawe-Taylor J. An Introduction to Support Vector Machines and Other Kernel-based Learning Methods. Cambridge, UK: Cambridge University Press, 2000.

[31] Kanal LN. Perceptrons. International Encyclopedia of the Social & Behavioral Sciences 2001; 11218-11221.

[32] Kingma DP, Ba J. Adam: A method for stochastic optimization. arXiv preprint arXiv:1412.6980, 2014.