11th International Scientific Conference
"Business and Management 2020"
May 7–8, 2020, Vilnius, LITHUANIA
Section: Finance: New Challenges, New Opportunities
http://www.bm.vgtu.lt

ISSN 2029-4441 / eISSN 2029-929X
ISBN 978-609-476-231-4
eISBN 978-609-476-230-7
https://doi.org/10.3846/bm.2020.558

INVESTIGATION OF CREDIT CARDS FRAUD DETECTION BY USING DEEP LEARNING AND CLASSIFICATION ALGORITHMS

Greta Pratuzaitė[1], Nijolė Maknickienė[2]

Department of Financial Engineering, Faculty of Business and Management,
Vilnius Gediminas Technical University, Saulėtekio al. 11, Vilnius, Lithuania
E-mails: [1]greta.pratuzaite@vgtu.lt; [2]nijole.maknickiene@vgtu.lt (corresponding author)

Received 16 April 2020; accepted 06 May 2020

Abstract. Criminal financial behaviour is a problem for both banks and newly created fintech companies. Credit card fraud detection becomes a challenge for any such company. The aim of this paper is to compare ability to detect credit card fraud by four algorithmic methods: Generalized method of moments, K-nearest neighbour, Naive Bayes classification and Deep learning. The deep learning algorithm has been tuned to select key parameters so that fraud detection accuracy is the best. Five recognition accuracy parameters and a cost calcualtions showed that the deep learning algorithm is the best fraud detection method compared to other classification algorithms. A financial company reduces losses and increases customer confidence by using fraud prevention technologies.

Keywords: fraud detection, classification, credit cards, FinTech, confusion matrix, loses, deep learning.

JEL Classification: G30, G40.

1. Introduction

A very serious problem in the banking sector is related to payment card fraud, which involves card fraud, card theft or fraudulent online payments. The emergence of new technologies offers additional opportunities for criminals to fraud. The use of credit cards is widespread and fraudulent use of this instrument has been on the rise lately. The financial losses caused by fraud affect not only banks but also individual customers. Fraud can also affect a bank's reputation, cause non-financial losses, which are somewhat more difficult to quantify in the short term, and may become more noticeable in the long run. The customer will no longer be able to trust his bank and will choose another more reliable competitor.

Prevention of fraud, which attempts to block fraudulent transactions and detect fraud, has existed since the emergence of credit card payments. Technologies that have been used to prevent fraud include the Address Verification System, the Card Verification Method, and the Personal Identification Number (Bhatla et al., 2003).

Modern banking uses a variety of fraud detection algorithms and machine learning methodologies. Classification algorithms assign each transaction to a particular risk group. Artificial intelligence algorithms determine the model based on databases. Most often, the model is a parametric function that predicts the likelihood of transaction fraud. The use of learning methods in fraud detection is a particularly effective tool because it allows for the detection of patterns in large-scale databases and each transaction is defined by many variables. Also, fraudulent transactions often correlate both in time and space.

The aim of this paper is to compare ability to detect credit card fraud of four algorithmic methods: Generalized method of moments, K-nearest neighbour, Naive Bayes classification and deep learning. Comparison of the methods reveals differences in classification accuracy and the financial benefit to the bank settlement company.

2. Studies of financial fraud and fraud detection techniques

Deceptive financial behaviour and attempts to recognize it go back a long way. Archaeological evidence from Mesopotamia and Egypt from 3300 to 3500 BFE. Shows that accountants or clerks visually recorded commercial monetary transactions using wet clay pills or papyrus to identify if the arrangement was unchanged (Palmer, 2017).

Modern society faces criminal financial activity not only in real life but also in virtual life. Companies pay a lot of attention to fraud detection. Lynch and Gomaa (2003) explored the impact of information technology on fraud prevention and

the potential for new forms of fraud. Andergassen (2008) investigated ability to reduce fraudulent behaviour of managers and studied the optimal managerial compensation package, which consist from shares and options. Author find a threshold level for the cost of fraud, above which stock-based compensation is optimal. Businesses are affected not only by fraud on the part of employees, but also by customers, suppliers or partners. Customer fraud include different types: payment, shoplifting, consuming services without paying, fraudulent returns, fare dodging, falsifying complaints, use of pirated software, and insurance fraud. Examining the scientific literature, we find a two-pronged approach to customer information: one company collects customer data and tries to use that data for fraud detection, while others accept the customer as anonymous. Different aspects of customers with profiles was investigated by Coma-Puig et al. (2016), Leite et al. (2016). Tseng (2019) examined the relationships among fraud types, moral intensity, fairness perception, demographic variables and customers' ethical attitudes and intentions toward insurance frauds. Another method of removing fraudulent behaviour was examined by Kalaiselvi et al. (2018), Zoldi and Xu (2019). These authors looked for anomalies in their own data. Garnefeld et al. (2019) investigated three payment characteristics that might evoke a need to balance accounts and thus increase fraud predilection: payment timing, payment schedule, and payment method. A multi-step investigation has uncovered the management of mental account perceptions as an innovative launch point for preventing and detecting customer fraud.

At the country level, fraudulent financial reporting is a major problem for each country's government. Fraud effects on countries economy are manifested in the following ways:

- undermines capital markets' core role of efficiently allocating resources (Amiram et al., 2018);
- cause of loss of trust and confidence of economic system;
- violates the database used for planning and forecasting;
- poses a threat to national security especially for young democracy countries;
- increases public debt and complicates its administration.

Carpenter and Reimers (2005) research applied the theory of planed behaviour to corporate managers' propensity to commit fraud in financial reporting decisions. Implementing ethical principles in a company can could reduce fraudulent financial reporting decisions. Fleming et al. (2016) compared public and private companies and reveal that public companies have stronger anti-fraud environments, are more likely to have frauds that involve timing differences, tend to experience larger frauds, have frauds that involve a larger number of perpetrators, and are less likely to have frauds that are discovered by accident. Van Erven et al. (2017) presents investigation on evidence of fraud in procurement processes. Antipova (2017) has provided an overview of research on government auditor's responsibility to prevent fraud in the public sector.

Each government and each company seeks to define, classify, and gauge the prevalence or investigates effective control techniques.

One of the oldest and most reliable ways to prevent fraud is to know people's psychology. Behaviour of management, including motivations, opportunities, fraud prevention, rationalizations for management to commit such fraud, has been extensively studied by researchers in finance (Rezaee, 2002; Petri et al., 2017; Yildirim et al., 2018).

Statistical fraud detection methods usually look for certain anomalies in the data: indicators excesses, changes in customer behaviour, sudden illogical actions (Bolton & Hand, 2002). Ahmed et al. (2017) investigated different methods of anomalies detection and concluded that nearest neighbour and clustering based approaches are more stable in big financial market data. Vat Fraud anomaly detection technique which examines the effect of sectoral differences was proposed by Vanhoeyveld et al. (2020).

With the emergence of innovative machine learning and artificial intelligence techniques, they have also been introduced to fraud detection. Ngai et al. (2011) study investigates the usefulness of Decision Trees, Neural Networks and Bayesian Belief Networks in the identification of fraudulent financial statements. Roy et al. (2018) investigate different Deep Learning topologies - from the general artificial neural network to topologies with built-in time and memory components such as Long Short-term memory. Raghavan and Gayar (2019) compared multiple machine learning methods such as k-nearest neighbour (KNN), random forest and support vector machines (SVM), while the deep learning methods such as autoencoders, convolutional neural networks (CNN), restricted Boltzmann machine (RBM) and deep belief networks (DBN). Park et al. (2019) propose a deep neural network that utilizes multi-modal inputs with an attention mechanism and a correspondence learning scheme. Unique attention mechanisms

create ability of better learning. Correspondence learning scheme, reveals intermodal relationships and thus can detect fraud inputs.

The use of artificial intelligence for credit card fraud detection often presents a problem of data asymmetry: there are many correct settlements compared to fraudulent transactions. Very good recognition accuracy results can be obtained but no financial gain. Kim et al. (2019) introduced the two types of misclassification, false alarms and missed frauds, that make it possible to evaluate this problem.

Our study compares different classification methods, takes into account data asymmetries, and evaluates the financial benefits if fraud is identified.

3. Classification methods and accuracy

From the Kaggle database system, a database related to credit card fraud was selected. These data are about credit card holder operations in Europe in September 2013. However, this dataset shows operations that have occurred within two days. A total of 492 fraudulent actions out of 284,807 transactions are committed. An experimental study analysed payment fraud using the Python programming language. Import the required libraries, apply algorithms to the selected models, and visualize the resulting data. The dataset is unbalanced as the positive class (fraud) accounts for 0.172% of all transactions. Because of the lack of confidentiality of key functions and other ancillary transaction information, the data has been transformed by Principal Component Analysis and for this reason, the data has a numerical value only (Lepoivre et al., 2016). This database consists of V1 to V28 variables that were obtained using the main component analysis function. A specific bank that would apply special algorithms in fraud detection would have complete information and could identify which attributes best represent fraud. This would allow the bank to take additional security measures on a specific basis, but in this case, due to confidentiality, the data has been transformed.

An important part of the research is to choose the appropriate grading methods to evaluate the accuracy of the grading.

The Confusion Matrix is a way of measuring machine learning classification, where the Output can be of two or more classes (see Figure 1). This matrix provides a visual representation of the resulting data based on 4 different combinations of predicted and actual (correct) values (Turban et al., 2014): False Positive (FP), True Positive (TP), False Negative (FN), True Negative (TN).

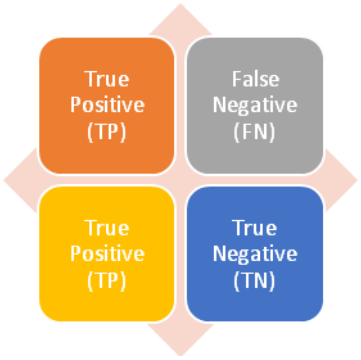

Figure 1. Confusion matrix
(source: compiled by authors)

Measures are usually using to determine classification accuracy (Turban et al., 2014):

- Accuracy refers to the ratio of correctly classified to total data and can be used when existing classes are balanced;

$$Accuracy = \frac{(TP+TN)}{(TP+TN+FP+FN)}, \quad (1)$$

where: *FP* – False Positive, *TP* – True Positive, *FN* – False Negative, *TN* – True Negative.

- Precision – can show how many predicted values are true results;

$$Precision = \frac{TP}{TP+FP}, \quad (2)$$

- Sensitivity (Recall) − can indicate what proportion of positive values were correctly predicted;

$$Recall = \frac{TP}{TP+FN}, \quad (3)$$

- The F1 score is needed when there is a balance between precision and recall and when the distribution of classes is uneven − a large number of actual negatives (Browlee, 2014).

$$F1 = 2\times\frac{Precision\times Recall}{Precision+Recall}, \quad (4)$$

- Area Under the Curve (AUC) − The Receiver Operating Characteristic (ROC) curve is used to solve classification tasks and show their performance. AUC is the area under the ROC curve and ROC is the probability curve. In order to evaluate the results of the model developed, the worst AUC exists at 0 and the best AUC at close to 1.

Gaussian Mixture Model (GMM) is a method of constructing estimates similar to maximum likelihood (Scherrer, 2007). This method uses assumptions about specific moments of random variables rather than assumptions about the entire distribution. Assumptions are called instantaneous conditions.

K-nearest neighbour's classification. The k-nearest-neighbour method starts from the random element, constantly selecting the nearest neighbour from the unselected. During testing, the number of nearest neighbours is changed. All data is decomposed into 80% for learning and 20% for testing. This method already includes all traits except time and class.

The naive Bayesian classifier method is a probabilistic classification method that is based on the Bayes rule. This classifier attempts to predict a class called the result class based on probabilities and also the probability of occurrence from learning data (Kiran et al., 2018). Such learning is very effective, fast and accurate. In addition, he estimates the parameters using very small training data that is used for classification.

Deep learning algorithm for classification. The sigmoidal activation function has been chosen for the deep learning algorithm because it helps to quickly classify the data, as its scales are from 0 to 1, which is applicable in fraudulent topics. Another activation feature of ReLU is its usability due to its faster learning process and the fact that it does not activate all neurons at the same time. If its input is negative, it will be converted to zero and the neuron will not be activated, indicating that only a few neurons are activated at a time, making the neural network small and more efficient. For the learning of artificial neural networks, large amounts of data are important, and the structure and basic hyper parameters can be properly determined. The parameters of this network are constantly changing to get the best recognition result. Another algorithm called "backpropogation", which helps to find the smallest error when using the learning speed, which is usually sought to be as low as possible, contributes to a more accurate result. Finally, all models of both machine learning and deep learning are compared against each other in terms of accuracy and the financial benefits that financial institutions can obtain if fraud is properly identified.

4. Comparison of algorithms in credit card fraud detection

Three data classification models have been selected and their results are compared with the fraud detection capabilities of the deep learning algorithm.

Gaussian Mixture Model (GMM). Fraud data is split equally between learning and testing, with non-fraud 90% for learning and 10% for testing. The model is trained with learning data and then tested with test data. Taking into account the Gaussian curves and the distribution of fraud and not fraud, four combinations of certain traits were selected and their accuracy indicators were calculated: accuracy (not fraud), accuracy (fraud), sensitivity (not fraud), sensitivity (fraud), F1 (not fraud), F1 (fraud), AUC (Table 1).

Table 1. Accuracy results by the GMM Model (source: compiled by authors)

	V3& V4	V9& V11	V14& V17	V10& V12
Precision	0.90	0.97	0.95	0.80
Recall	0.21	0.15	0.72	0.43
F1	0.34	0.25	0.81	0.56
AUC	0.20	0.15	0.68	0.34

The results obtained allowed one pair of traits V14&V17 to be selected with the highest accuracy and expected the best recognition result. A real bank that knows what these features are can look at these indicators. The fraud detection classification matrix was obtained specifically for these indicators (Figure 2).

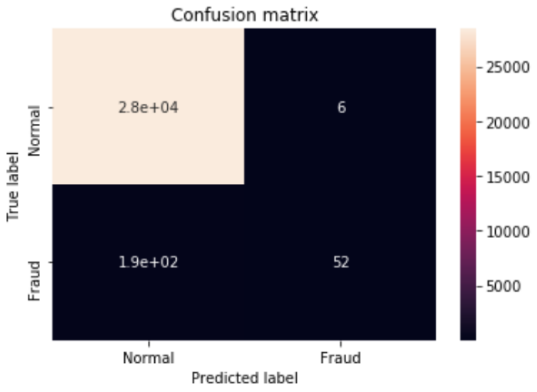

Figure 2. Confusion matrix of GMM model (source: compiled by authors)

Confusion matrix results shows bog number of missed frauds (190) with comparison of detected fraud (52).

K-nearest neighbour method. 0.8 parts of the data are devoted to learning and the rest to testing. During the study, the number of closest neigh-

bours was changed and the extent to which it affects the accuracy measures was monitored. The overall classification accuracy is very high after performing all four tests with different numbers of neighbours, equal to 0.99, which is an excellent result but should not be relied upon completely (see Table 2). The sensitivity result is in all cases lower than the accuracy, but still quite high overall. The AUC score is highest when one neighbour is selected and lowest when ten is selected. And the F1 measure, which combines accuracy and sensitivity, is above 0.7, which represents the average rating. Interestingly, with a sharp increase in the number of neighbours, the measure and accuracy of F1 gradually decrease.

Table 2. Accuracy results by the k-nearest neighbour method (source: compiled by authors)

	1 neighbour	5 neighbours	10 neighbours	20 neighbours
Accuracy	0.999	0.999	0.999	0.999
Precision	0.780	0.873	0.9	0.794
Recall	0.771	0.729	0.636	0.683
F1	0.778	0.795	0.746	0.735
AUC	0.895	0.822	0.701	0.838

There is also customizable confusion matric to evaluate this approach, which show how the model recognizes payments with and without fraud.

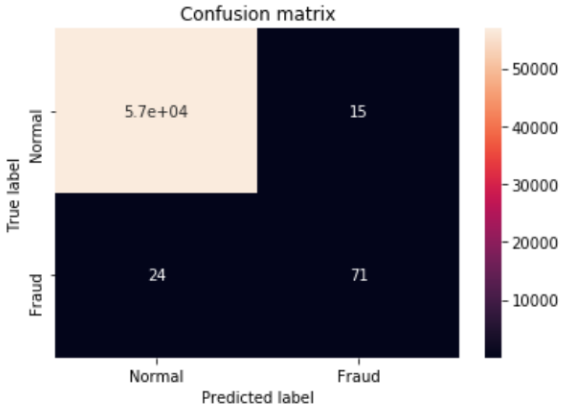

Figure 3. Confusion matrix of k-nearest neighbour model (source: compiled by authors)

The results (Figure 3) show that 71 cases of fraud were well recognized, missed 24, and false alarms 15.

The naive Bayes model was also chosen to detect fraud. This model also monitors the relationship to time and payment amounts, but ultimately only V1-V28 features are used for further analysis. Like other models, this data is divided into 0.2 for testing and 0.8 for learning.

Table 3. Accuracy results by the naive Bayes Model (source: compiled by authors)

	Naive Bayes method
Accuracy	0.9764
Precision	0.0587
Recall	0.8469
F1	0.1099
AUC	0.9632

The overall classification accuracy of the model is quite high, reaching 0.98, but the precision is extremely low (see Table 3). F1 also shows more low accuracy, reaching barely 0.11. Although the AUC score is very high at 0.96, it only shows that the model is less reliable than the one previously analysed. The error matrix for this model, based on test data, shows good recognition of fraud (55 cases), messed 43 and false alarms 13 (Figure 4).

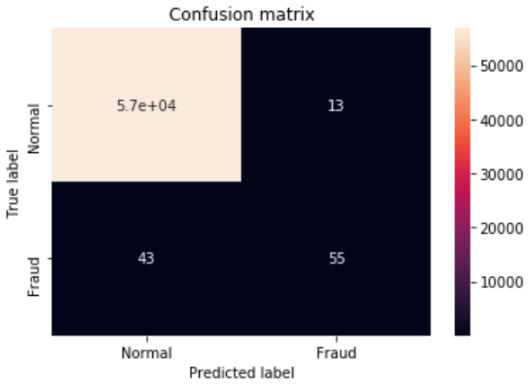

Figure 4. Confusion matrix of naïve Bayes model (source: compiled by authors)

Deep learning algorithm. Fraud detection data is divided into two parts: 80% for learning and 20% for testing. Using a deep neural network algorithm and training data, a classifier is constructed. The model is also applicable to test data. Once the classifier is constructed and tested using test data, it is necessary to check its accuracy. Primary neuron weights are unknown and randomly selected using the "random" function, and the number of layers and the number of neurons are changed au-

tomatically. The rate of learning is also determined by the lower it is, the better the neural network learns. The study attempts to increase the number of iterations to make learning longer and possibly more effective. More neurons are better, but sometimes re-learning can occur and the result may begin to deteriorate with such data. The fraud detection accuracy data of the harmonized deep learning algorithm are presented in the Table 4.

Table 4. Accuracy results by the deep learning model (source: compiled by authors)

	Deep learning
Accuracy	0.9995
Precision	0.87
Recall	0.83
F1	0.85
AUC	0.72

The estimated total measure of accuracy has a high degree of accuracy, other measures too. The F1 score is also relatively high compared to other grading methods. The AUC score is 0.72, which also suggests good accuracy.

Compared to other methods, confusion matrix represents the best result. It was mistaken for 30 times misclassifying fraud and not fraud.

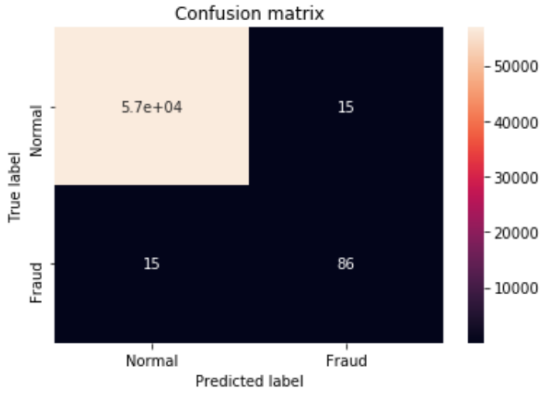

Figure 5. Confusion matrix of deep learning model (source: compiled by authors)

Confusion matrix (Figure 5) shows the good recognition of fraud in 86 cases, missed − 15 and false alarm − 15.

Comparison of the confusion matrices (see Table 5) shows that the best classification accuracy results can be achieved with deep learning model, with little lag behind k-nearest neighbour's classification algorithm. Gaussian Mixture Model and naïve Bayes model do not recognize a relatively high level of fraud, although the Gaussian Mixture Models false alarms number is the lowest.

Table 5. Comparison of accuracy of classification methods (source: compiled by authors)

	Detected fraud	Missed fraud	False alarm
Gaussian Mixture Model	53	190	6
K-nearest neighbours classification	71	24	15
Naive Bayes model	56	43	13
Deep learning	86	15	15

The general accuracy indicators of most grading methods have had fairly good results, but other criteria that make it easier to compare which model is best have to be considered.

It is important for banks to have such models and use them, as they create customer confidence and reduce the risk of potential unfair events that could have severe consequences for both customers and the financial institution. The table below shows the overall accuracy of all models and the potential financial benefits (see Table 6).

Table 6. Comparison of financial benefit of classification methods (source: compiled by authors)

	Total accuracy	Financial benefit (EUR)
Gaussian Mixture Model	0.81	36918,6
K-nearest neighbours classification	0.765	47801,7
Naive Bayes model	0.110	6614,1
Deep learning	0.999	60097,7

The financial benefit was calculated on the basis of fraud detection and its total amount. The greater the pattern recognition, the greater the financial benefit. If the pattern recognition is low, there is a high risk that the bank will suffer financial losses and will not notice fraud.

5. Conclusions

There are quite a few algorithms used to detect credit card fraud. Most often they perform a classification function, such as the Gaussian Mixture Model, decision tree, the k-nearest neighbour method, The naive Bayes model. The chosen deep learning is distinguished by its different structure, consisting of weights, layers, number of neurons and the ability to learn if there is enough data.

The research of the chosen methods aimed to apply the most suitable parameters, to determine the appropriate architectures for the best recognition result. The results showed that deep learning through neural networks achieved the greatest recognition. Its recognition was 99.9 percent. Deep learning tends to be more responsive to new data and to perform more than just a classification function than other methods.

All models have been tested in the same database, but each model has a different way of sampling, which makes comparison difficult. The deep learning algorithm showed the best fraud detection results (86), missed fraud (15) and thus the highest financial gain (60097 euros). The following result belongs to the K-nearest neighbour's classification method − 71, 24, 47801 respectively.

The study has several limitations. The data in the database is coded, so we can't recognize which data is more important in fraud detection. The data we selected for our study represented multiple days of payments, so the accuracy we get may be highly error prone. However, if the data were semi-annual or annual and targeted methods were used, the accuracy would be somewhat higher. When calculating the financial benefit, it would also make sense to estimate the cost of the resources needed. The comparison of classification methods is complicated by the fact that the methods for data selection and accuracy assessment of all methods are very different.

Disclosure statement

Authors not have any competing financial, profession-al, or personal interests from other parties.

References

Ahmed, M., Choudhury, N., & Uddin, S. (2017, July). Anomaly detection on big data in financial markets. In *Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2017* (pp. 998−1001). https://doi.org/10.1145/3110025.3119402

Amiram, D., Bozanic, Z., Cox, J. D., Dupont, Q., Karpoff, J. M., & Sloan, R. (2018). Financial reporting fraud and other forms of misconduct: a multidisciplinary review of the literature. *Review of Accounting Studies*, *23*(2), 732−783. https://doi.org/10.1007/s11142-017-9435-x

Andergassen, R. (2008). High-powered incentives and fraudulent behavior: Stock-based versus stock option-based compensation. *Economics Letters*, *101*(2), 122−125. https://doi.org/10.1016/j.econlet.2008.07.009

Antipova, T. (2017, June). Fraud prevention by government auditors. In *2017 12th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1−6). IEEE. https://doi.org/10.23919/CISTI.2017.7976024

Bhatla, T. P., Prabhu, V., & Dua, A. (2003). Understanding credit card frauds. *Cards Business Review*, *1*(6).

Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical Science*, 235−249. https://doi.org/10.1214/ss/1042727940

Carpenter, T. D., & Reimers, J. L. (2005). Unethical and fraudulent financial reporting: Applying the theory of planned behavior. *Journal of Business Ethics*, *60*(2), 115−129. https://doi.org/10.1007/s10551-004-7370-9

Coma-Puig, B., Carmona, J., Gavalda, R., Alcoverro, S., & Martin, V. (2016, October). Fraud detection in energy consumption: A supervised approach. In *2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA)* (pp. 120−129). IEEE. https://doi.org/10.1109/DSAA.2016.19

Fleming, A. S., Hermanson, D. R., Kranacher, M. J., & Riley Jr, R. A. (2016). Financial reporting fraud: Public and private companies. *Journal of Forensic Accounting Research*, *1*(1), A27-A41. https://doi.org/10.2308/jfar-51475

Garnefeld, I., Eggert, A., Husemann-Kopetzky, M., & Böhm, E. (2019). Exploring the link between payment schemes and customer fraud: a mental accounting perspective. *Journal of the Academy of Marketing Science*, *47*(4), 595−616. https://doi.org/10.1007/s11747-019-00653-x

Kalaiselvi, N., Rajalakshmi, S., Padmavathi, J., & Karthiga, J. B. (2018, March). Credit card fraud detection using learning to rank approach. In *2018 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC)* (pp. 191−196). IEEE. https://doi.org/10.1109/ICCPEIC.2018.8525171

Kim, E., Lee, J., Shin, H., Yang, H., Cho, S., Nam, S. K., & Kim, J. I. (2019). Champion-challenger analysis for credit card fraud detection: Hybrid ensemble and deep learning. *Expert Systems with Applications*, *128*, 214−224. https://doi.org/10.1016/j.eswa.2019.03.042

Kiran, S., Kumar, N., Guru, J., Katariya, D., Kumar, R., & Sharma, M. (2018). Credit card fraud detection using Naïve Bayes model based and KNN classifier. *International Journal of Advance Research, Ideas and Innovations in Technoloy*, *4*(3).

Leite, R. A., Gschwandtner, T., Miksch, S., Gstrein, E., & Kuntner, J. (2016, June). Visual analytics for fraud detection: focusing on profile analysis. In *EuroVis (Posters)* (pp. 45−47). https://doi.org/10.1109/VAST.2015.7347678

Lepoivre, M. R., Avanzini, C. O., Bignon, G., Legendre, L., & Piwele, A. K. (2016). Credit card fraud detection with unsupervised algorithms. *Journal of Advances in Information Technology*, *7*(1), 34−38. https://doi.org/10.12720/jait.7.1.34-38

Lynch, A., & Gomaa, M. (2003). Understanding the potential impact of information technology on the susceptibility of organizations to fraudulent employee behavior. *International Journal of Accounting Information Systems*, *4*(4), 295−308. https://doi.org/10.1016/j.accinf.2003.04.001

Ngai, E. W., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, *50*(3), 559−569. https://doi.org/10.1016/j.dss.2010.08.006

Palmer, N. S. (2017). Euclid. *Ancient history encyclopaedia*. https://www.ancient.eu/writing/

Park, J., Kim, M. H., Choi, S., Kweon, I. S., & Choi, D. G. (2019, January). Fraud detection with multi-modal attention and correspondence learning. In *2019 International Conference on Electronics, Information, and Communication (ICEIC)* (pp. 1−7). IEEE. https://doi.org/10.23919/ELINFOCOM.2019.8706354

Petri, D., Kohout, G., Nader, G., & Mayerhofer, M. (2017). *U.S. Patent No. 9,785,988*. U.S. Patent and Trademark Office.

Raghavan, P., & El Gayar, N. (2019, December). Fraud detection using machine learning and deep learning. In *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)* (pp. 334−339). IEEE. https://doi.org/10.1109/ICCIKE47802.2019.9004231

Rezaee, Z. (2002). *Financial statement fraud: prevention and detection*. John Wiley & Sons.

Roy, A., Sun, J., Mahoney, R., Alonzi, L., Adams, S., & Beling, P. (2018, April). Deep learning detecting fraud in credit card transactions. In *2018 Systems and Information Engineering Design Symposium (SIEDS)* (pp. 129−134). IEEE. https://doi.org/10.1109/SIEDS.2018.8374722

Scherrer, B. (2007, February). *Gaussian Mixture Model classifiers* (Lecture notes). http://www.medialab.bme.hu/medialabAdmin/uploads/VITMM225/GMMScherrer07.pdf

Tseng, L. M. (2019). Customer insurance frauds: the influence of fraud type, moral intensity and fairness perception. *Managerial Finance*, *45*(3), 452−467 https://doi.org/10.1108/MF-04-2018-0162

Turban, E., Sharda, R., & Delen, D. (2014). *Business intelligence and analytics: systems for decision support*. Pearson Higher Ed.

Van Erven, G. C., Holanda, M., & Carvalho, R. N. (2017, April). Detecting evidence of fraud in the brazilian government using graph databases. In *World conference on information systems and technologies* (pp. 464−473). Springer. https://doi.org/10.1007/978-3-319-56538-5_47

Vanhoeyveld, J., Martens, D., & Peeters, B. (2020). Value-added tax fraud detection with scalable anomaly detection techniques. *Applied Soft Computing*, *86*, 105895. https://doi.org/10.1016/j.asoc.2019.105895

Yildirim, M. Y., Ozer, M., & Davulcu, H. (2018, May). Cost-sensitive decision making for online fraud management. In *IFIP International Conference on Artificial Intelligence Applications and Innovations* (pp. 323−336). Springer. https://doi.org/10.1007/978-3-319-92007-8_28

Zoldi, S. M., & Xu, H. (2019). *U.S. Patent application No. 15/697,375*.