Introducing a heuristic method for combining fraud evidence based on outlier detection

(Mehrdad Kargari m_kargari@modares.ac.ir)

(Ali Mohammad Naderi am.naderi@qiau.ac.ir)

(Zahra Eskandari eskandarinet@gmail.com)

(Hamed Mirashk mirashk@caspco.ir)

(Abdollah Eshghi a.eshghi@modares.ac.ir)

Abstract: Huge amount of money is lost due to fraud each year, and fraud is a main obstacle for extending the electronic commerce. The dearth of labeled data is a reason for conducting fraud detection studies via unsupervised methods. However unsupervised methods like outlier detection methods cannot leading up to acceptable results in fraud detection systems. In this paper a heuristic method is introduced which combines the evidence gained from an outlier detection method based on their appropriate weights. At first the behavioral features of the card owners are extracted and a proportional weight is given to each feature's trend. Then by applying a fuzzy method on each behavioral trend, the outliers are detected and finally the results of the outlier detection method for each feature which is the deviation of each feature from the previous normal trends are combined according to the given weight to each feature. After applying the introduced method on a real world data, we showed that by applying outlier detection on each feature and holding its result as an evidence and combining them based on their weights, rather than more accurate results the speed will improve remarkably.

Key words: fraud detection, fuzzy, outlier, heuristic method

1 Introduction

Fraud has become a main obstacle in electronic commerce world and several statistics are reported on the number and volume of fraud in different countries and for different businesses. Just for payment cards, it is estimated that billions of dollars of revenue are lost around the world [1]. A report published by the European Central Bank in 2014 [2], showed an increase of 14.8% compared to 2011 and again according to Nilson Report [3], fraud in 2015 had an increase about 20% compared to 2014. Frauds have a an increasing trend and as stated in [4], the organizations in USA lose about 7% of their revenues due to fraud. Accordingly, online fraud detection is growing in complexity and demand, and its tools are being used for risk-based authentication and new account fraud prevention [5].

Fraud detection systems are always facing with several challenges including constantly changing behavior of customers [6], having no best practice algorithm or method [7], skewed datasets [8],and having no labeled datasets [9]. Machine learning methods like deep learning, ensemble methods, unsupervised and supervised methods have good potentials for analyzing data and also for fraud detection [5]. Supervised methods are straight-forward to fraud detection and their results are more understandable, but they have two critical challenges if applied solely to fraud detection. First, in most cases, especially in banking sectors, there is no labeled data to apply supervised algorithms on them and [9], second, it is not an easy task to find distinctive labels because of the uncertainties and ambiguities in the supervision or labels [10]. Using supervised and unsupervised methods together can improve the results remarkably and since in most of the cases there is no labeled datasets, focusing on unsupervised and semi-supervised methods is of great importance.

Most of the unsupervised and semi-supervised methods are based on outlier detection [7], but fraud detection is a labor intensive work and finding fraud cases are not as easy to find with a simple outlier detection method. In this paper we extracted the trend of normal behavior of customers. Then based on each of these extracted normal trends the deviation of each trend is calculated and the outlier features are determined. Finally, by combining the calculated deviation using a heuristic method the final result is calculated.

The reminder of the paper is organized as follows: in section 2, the literature review is presented. Section 3 is about the introduced heuristic fusion approach. In section 4 the results are presented and finally the conclusion is in section 5.

2 Literature Review

Practical implementation of fraud detection systems are rarely reported [11]. Because of the dearth of labeled data, any fraud detection system must have an unsupervised component [10] and most of the fraud detection techniques applied a concept referred to as outlier detection [7]. As defined by Hawkins [12], Outlier is an observation that is so different from other observations so that it appears to have been generated by a different mechanism.

In fraud detection, the problem is more complicated; because not necessarily all the outliers are frauds and it seems that outlier detection employed alone does not yield satisfactory results [10].

Supervised and unsupervised methods for fraud detection:

As mentioned previously three main categories of fraud detection techniques are supervised, unsupervised and semi-supervised techniques. Supervised techniques can be categorized as classification and regression algorithms [9]. Some classification algorithms which are used in fraud detection systems are artificial neural network [8], [13]–[19], Artificial immune systems [20], [21], K-nearest neighbors [22], [23], trees [24]–[26], logistic regression [27], Naïve–Bayes [28], [29] and support vector machine (SVM) techniques [30]. Linear regression, simple regression and logistic regression are examples of regression algorithms. In recent years deep learning algorithms are also used for fraud detection [31]–[33]. The main categories for unsupervised algorithms are clustering

algorithms [34]–[36] and dimensionality reduction algorithms such as: Principal component analysis (PCA) [37]. Semi-supervised learning lies between Supervised and Unsupervised learning since it involves a small number of labelled samples and a large number of unlabeled samples [9].

The semi-supervised fraud detection methods are based on profiling methods. In these methods the normal behaviors of customers (for example the card owners) are profiled and then the new behaviors are estimated based on them. Fawcett and Provost have used the profiling method for credit card fraud detection [38], they tried to detect suspicious changes in user behavior by using a rule-learning program to uncover indicators of fraudulent behavior from a large database of customer transactions [38]. Rather than profiling of normal behaviors, one can make profiles of fraudulent behaviors too. In [39]–[41] the historical behaviors of fraudsters are profiled. This help the fraud detection system to detect fraudulent behaviors as early as possible. In [42] a window time of fraud-less account activity is regarded as a base for calculating user profiles. The trend of spending changes in customer behavior is detected by break point analysis in [43].

The behavioral profile of a customer is made of several features and the trend of these features make the overall behavior trend for that customer. The distinction between a normal behavior and a fraudulent one can be recognized by estimating the deviation of each of these features from their normal trends. The normal trend is composed of a set of aggregated features. These aggregated features are not the same or at least do not have the same weight for all customers [10] and hence labeling a transaction as an outlier or as a normal transaction is a challenge. For this purpose, the trends of all features must be fused. The process for extracting aggregated features is described in [44], [45] and the process of infusing several evidence is used previously by Panigrahi et al; in [46] and later by Eshghi and Kargari in [47]. In [46], the dempster-shafer method is used while in [47] the authors have used a MCDM approach based on intuitionistic fuzzy set. In this paper a heuristic method is proposed for the fusion of several evidence and we showed that it has an acceptable precision with a remarkable improve in speed compared to the fusion methods introduced in [46] and [47].

2.1 Extraction of Trends

The extraction process of trends is shown in Figure 1. The total number of the extracted trends is 112 trends (5*4*5 + 4*3). For example, one of the extracted trends is as follow: “the trend which represents the hourly number of purchases of a customer through the internet channel”. For each trend a fuzzy function is calculated. The fuzzy functions show the margins of outliers for each trends of the customer’s behavior. In this paper the extracted fuzzy functions are based on the method introduced in [7].

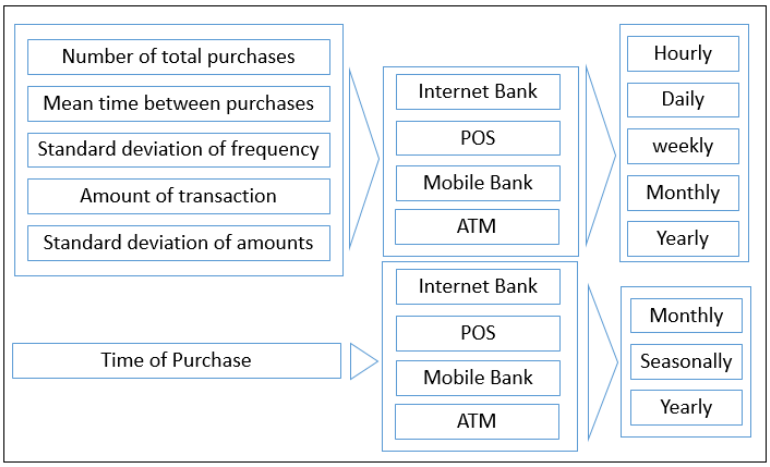

Figure 1 Extraction Process of Trends

The representation of the fuzzy functions for trends of amount/count of purchases and trends of time of purchases are shown in Figure 2 and Figure 3 respectively. These fuzzy functions are based on soft (S) and hard (H) thresholds. For example, if the count of purchases in a trend is less than S then its risk is 0, if the count is more than H then its risk is 1, if the count is between S and H then the risk is a point on the line that connects S and H.

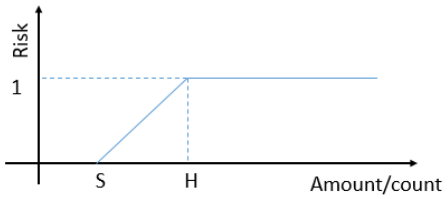

Figure 2 Fuzzy function for the trends of amount/count of purchases [7]

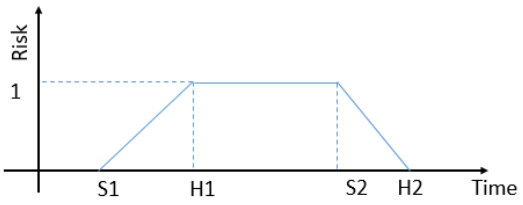

Figure 3 Fuzzy function for the trends of time of purchases [7]

3 Fusion of Evidence

In this paper the trends are categorized as strict and non-strict trends. Strict trends are those trends that any deviation from them means that some anomaly has occurred in the transaction. For example, the time interval between two transactions must not be less than 10 seconds. In other hand, deviation from non-strict trends does not necessarily means an anomaly and they must be treated in different way. Among the strict trends, the result of the trend which has the maximum risk will be selected.

The weights of the trends are not the same for all customers and their dominant features are different. A dominant feature or a dominant behavior is an aspect of a customer behavior which its standard deviation is 0 or very low. Among the extracted trends, those which are dominant, are assigned 1 to their weights. In order to determine the dominant trends, a sequence of previous calculated risks is regraded. Since the normal trends are stored in the database, we expect very low risks for normal transactions. If the previous calculated risks for a special trend of genuine transactions are high, then we conclude that this trend is not a dominant trend for that customer and hence the associated weight is low. The process of assigning weights to dominant and non-dominant trends is shown in and Figure 5.

As shown in Figure 5, if the previous calculated risks of any trends for genuine transactions is more than 0, then its related weight in next transaction will be low and hence if all the previous calculated risks are 1 for that trend, then its related weight will be 0. By this way, the features are selected based on their weights and some sort of personalized feature selection is applied for each customer.

for each (trends in $R_1$to R_n){

$previou\_risks(R_i) = \{R_{i_{t1}}, R_{i_{t2}}, \dots, R_{i_{tn}}\}$

$std(R_i) = standard\_deviation\_of\,(previou - risks(R_i))$

$if\,(|std(R_i)| \leq \epsilon)\ then\ R_i\ id\ dominant\ trend$

}

Figure 4 Determine if a trend is dominant or not

for each (trends in $R_1$to R_n){

$if(R_i\ is\ dominant)\ then\ w_{R_i} = 1$

$else\ w_{R_i} = 1 - Mean(previou - risks(R_i))$

}

Figure 5 Assigning weights to trends

After determining strict and non-strict trends and assigning related weights to non-strict trends, the fusion of trends will be done. As mentioned previously, each trends act as an evidence for the fraud detection system. We determine the final state of transactions (fraud or not-fraud) by combining of all the evidence as shown in Figure 6.

The deviations of a new arrived transaction from its normal trends is estimated using the fuzzy functions introduced in previous section. Here we use deviation and risk interchangeably. Then using the function introduced in **Error! Reference source not found.**, the dominant trends are determined and for each of them, the associate weight is assigned by applying the function introduced in Figure 5 and the weighted average of the non-dominant trends deviations (risks) is calculated. In order to tune the estimated weighted average, we multiply it by a factor (sf). This factor is calculated as below:

$$\mathbf{sf} = \frac{\mathbf{e^x - 1}}{\mathbf{e^x}} \qquad \text{Equation 1}$$

in Equation 1, x is the number of the trends which their risks are more than a special threshold (th) . The threshold is determined empirically by the experts. Its main purpose is to discriminate between cases where all of their trends have risks more than the threshold and cases where just a few number of trends have risks more than the threshold. Finally as shown in Figure 6, using the MAX function, the final risk is estimated. The final risk is a number between 0 and 1. we again can assign a threshold to decide if a transaction is fraud or no-fraud. This threshold can be selected based on a tradeoff between false alarm rates and true detected cases as we show in next section.

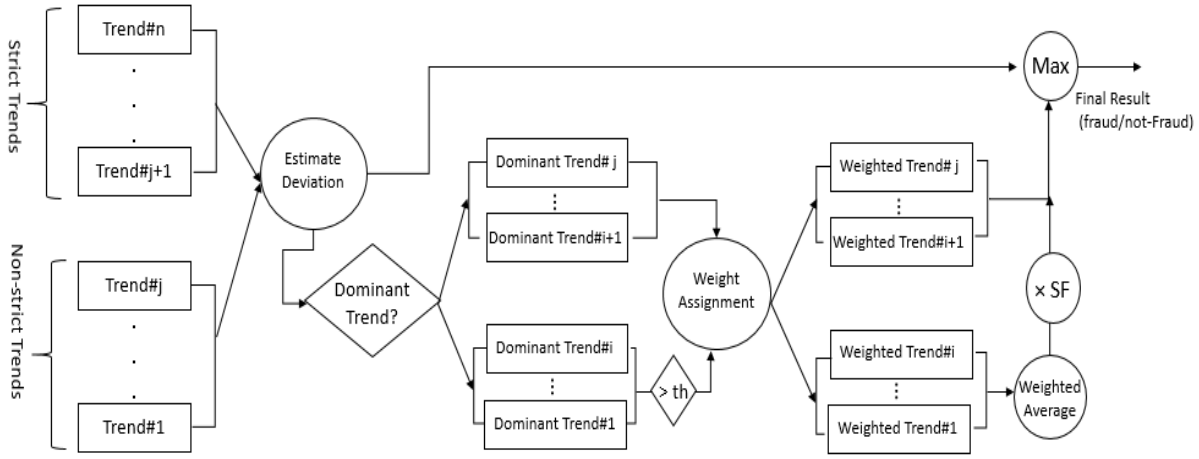

Figure 6 The process of fusing of trends

The process shown in Figure 6, can be repeated for all levels. For example, in banking transactions, 3 different levels can be defined (card level, account level, customer level).

4 Results

We used the dataset that was used in [47]. It was a one-year genuine transactional data of an Iranian private bank from February 2015 to February 2016. There are 12 raw features for each transaction of the dataset. Besides, in [47], a synthetic method has been used for generating fraudulent transactions. The synthetic method was introduced in [46].

True positives (TP) and false positives (FP) are used as standard metrics for evaluating the system. True positives (TP) are the fraudulent transactions that are detected by the system and false positives (FP) are the genuine transactions which are detected as fraudulent transactions mistakenly [47]. The fusion results of the proposed method is compared with the fusion results of [46] and [47]. In [46], the fusion is done by using of dempster-shafer method and in [47], the fusion is done by using an intuitionistic fuzzy approach. The process of calculating results and comparing them with 3 different methods is shown in Figure **7**.

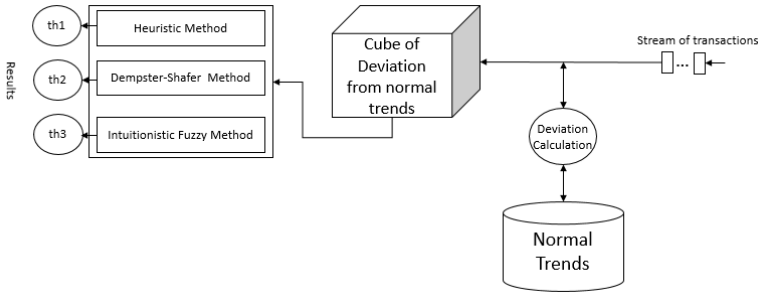

Figure 7 Block Diagram of the model

The final result for each fusion method is based on a threshold. Different thresholds lead to different FP and TP rates. A comparison of FP and TP for different thresholds of each method is shown in Table 1 and the graphical view is shown in Figure **8**.

Table 1 Variation of TP and FP of intuitionistic fuzzy, Dempster–Shafer and heuristic methods for different thresholds.

Th	Heuristic_FP	Heuristic _TP	DS_FP	DS_TP	MC_FP	MC_TP
0	0.7563	0.97	0.6101	0.98	0.6365	0.97
0.1	0.6854	0.97	0.5274	0.97	0.5659	0.97
0.2	0.5502	0.96	0.4752	0.97	0.4877	0.96
0.3	0.4781	0.95	0.3184	0.94	0.3692	0.95
0.4	0.3864	0.93	0.1865	0.92	0.2121	0.94
0.5	0.2341	0.88	0.1074	0.84	0.1269	0.91
0.6	0.1114	0.81	0.0841	0.79	0.0898	0.88
0.7	0.0983	0.78	0.0643	0.68	0.0576	0.83
0.8	0.0476	0.66	0.0116	0.54	0.0101	0.73
0.9	0.0107	0.53	0.0076	0.49	0.0068	0.57
1	0.0084	0.32	0.0021	0.31	0.0019	0.46

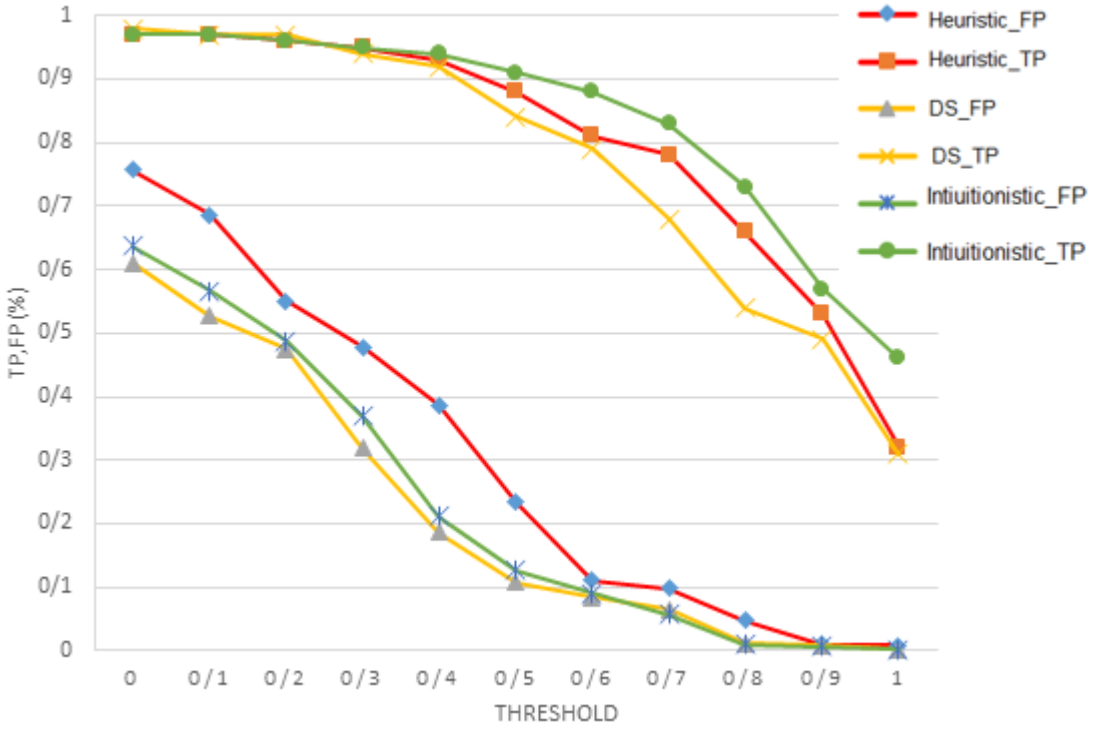

Figure 8 Variation of TP and FP of intutionistic fuzzy, Dempster–Shafer and heuristic methods for different thresholds.

High rate of TP and low rate of FP is more preferable in fraud detection systems. As we notice from Figure 8 and Table 1, the intuitionistic method has more TP rates (73%) compared to the heuristic (66%) and dempster-shafer (54%) methods when the threshold is 0.8.

Although the heuristic method is not better than the intuitionistic fuzzy method based on TP and FP factors, it outperforms the intuitionistic fuzzy and dempster-shafer methods according to the number of transactions that it can manipulate per second (TPS). TPS is another important factor of fraud detection systems, especially in banking systems [47]. By running these three methods on a same computer system, their TPS is shown in Figure **9**.

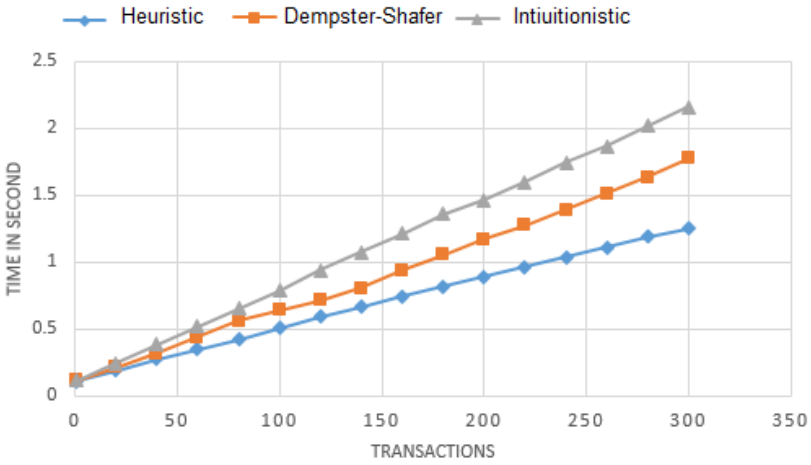

Figure 9 The TPS of Heuristic, Dempster-Shafer and Intuitionistic Fuzzy methods

5 Conclusion

In this paper a heuristic approach for combining different evidence of fraud is introduced and its results was compared with 2 other approaches: intuitionistic fuzzy approach and dempster-shafer approach. Although its speed is more acceptable than the others, its precision is lower than the intuitionistic fuzzy and it needs to be improved.

References

[1] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," *Decis. Support Syst.*, vol. 50, no. 3, pp. 602–613, Feb. 2011.
[2] European Central Bank, "Technical Report," 2014.
[3] "Nilson Report," 2016.
[4] R. Nisbet, G. Miner, and K. Yale, "Chapter 15 - Fraud Detection," in *Handbook of Statistical Analysis and Data Mining Applications (Second Edition)*, R. Nisbet, G. Miner, and K. Yale, Eds. Boston: Academic Press, 2018, pp. 289–302.
[5] Gartner, "Market Guide for Online Fraud Detection," 2018.
[6] M. E. Edge and P. R. Falcone Sampaio, "A survey of signature based methods for financial fraud detection," *Comput. Secur.*, vol. 28, no. 6, pp. 381–394, Sep. 2009.
[7] A. Eshghi and M. Kargari, "Detecting frauds using customer behavior trend analysis and known scenarios," *Int. J. Ind. Eng. Prod. Res.*, vol. 29, no. 1, pp. 91–101, Mar. 2018.
[8] S. Wang, "A Comprehensive Survey of Data Mining-Based Accounting-Fraud Detection Research," in *2010 International Conference on Intelligent Computation Technology and Automation (ICICTA)*, 2010, vol. 1, pp. 50–53.
[9] A. Abdallah, A. Maarof, and M. Aizaini Maarof, "Fraud detection system: A survey," *J. Netw. Comput. Appl.*, vol. 68, pp. 90–113, Jun. 2016.

[10] A. Eshghi and M. Kargari, "Introducing a New Method for the Fusion of Fraud Evidence in Banking Transactions with Regards to Uncertainty," *Expert Syst. Appl.*, Nov. 2018.
[11] M. Carminati, R. Caron, F. Maggi, I. Epifani, and S. Zanero, "BankSealer: A decision support system for online banking fraud analysis and investigation," *Comput. Secur.*, vol. 53, pp. 175–186, Sep. 2015.
[12] D. Hawkins, *Identification of Outliers*. Springer Netherlands, 1980.
[13] Ghosh and Reilly, "Credit card fraud detection with a neural-network," in *1994 Proceedings of the Twenty-Seventh Hawaii International Conference on System Sciences*, 1994, vol. 3, pp. 621–630.
[14] J. R. Dorronsoro, F. Ginel, C. Sgnchez, and C. S. Cruz, "Neural fraud detection in credit card operations," *IEEE Trans. Neural Netw.*, vol. 8, no. 4, pp. 827–834, Jul. 1997.
[15] R. Brause, T. Langsdorf, and M. Hepp, "Neural Data Mining for Credit Card Fraud Detection," in *Proceedings of the 11th IEEE International Conference on Tools with Artificial Intelligence*, Washington, DC, USA, 1999, pp. 103–.
[16] Maes, K. Tuyls, B. Vanschoenwinkel, and B. Manderick, "Credit card fraud detection using Bayesian and neural networks," *Proc. 1st Int. Naiso Congr. Neuro Fuzzy Technol.*, 2002.
[17] H.-C. Kim, S. Pang, H.-M. Je, D. Kim, and S. Yang Bang, "Constructing support vector machine ensemble," *Pattern Recognit.*, vol. 36, no. 12, pp. 2757–2767, Dec. 2003.
[18] M. Syeda, Y.-Q. Zhang, and Y. Pan, "Parallel granular neural networks for fast credit card fraud detection," in *2002 IEEE World Congress on Computational Intelligence. 2002 IEEE International Conference on Fuzzy Systems. FUZZ-IEEE'02. Proceedings (Cat. No.02CH37291)*, 2002, vol. 1, pp. 572–577 vol.1.
[19] A. Srivastava, A. Kundu, S. Sural, and A. Majumdar, "Credit Card Fraud Detection Using Hidden Markov Model," *IEEE Trans. Dependable Secure Comput.*, vol. 5, no. 1, pp. 37–48, Jan. 2008.
[20] N. Soltani Halvaiee and M. K. Akbari, "A Novel Model for Credit Card Fraud Detection Using Artificial Immune Systems," *Appl Soft Comput*, vol. 24, no. C, pp. 40–49, Nov. 2014.
[21] N. F. Ryman-Tubb, P. Krause, and W. Garn, "How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark," *Eng. Appl. Artif. Intell.*, vol. 76, pp. 130–157, Nov. 2018.
[22] Y. Li, C. Yan, W. Liu, and M. Li, "A principle component analysis-based random forest with the potential nearest neighbor method for automobile insurance fraud identification," *Appl. Soft Comput.*, vol. 70, pp. 1000–1009, Sep. 2018.
[23] S. Nami and M. Shajari, "Cost-sensitive payment card fraud detection based on dynamic random forest and k-nearest neighbors," *Expert Syst. Appl.*, vol. 110, pp. 381–392, Nov. 2018.
[24] Y. Sahin, S. Bulkan, and E. Duman, "A cost-sensitive decision tree approach for fraud detection," *Expert Syst. Appl.*, vol. 40, no. 15, pp. 5916–5923, Nov. 2013.
[25] M. P. Bach, K. Dumičić, B. Žmuk, T. Ćurlin, and J. Zoroja, "Internal fraud in a project-based organization: CHAID decision tree analysis," *Procedia Comput. Sci.*, vol. 138, pp. 680–687, Jan. 2018.

[26] Y.-J. Chen, W.-C. Liou, Y.-M. Chen, and J.-H. Wu, "Fraud detection for financial statements of business groups," *Int. J. Account. Inf. Syst.*, Dec. 2018.
[27] Y. Sahin and E. Duman, "Detecting credit card fraud by ANN and logistic regression," in *2011 International Symposium on Innovations in Intelligent Systems and Applications*, 2011, pp. 315–319.
[28] Y. Ma, S. Liang, X. Chen, and C. Jia, "The Approach to Detect Abnormal Access Behavior Based on Naive Bayes Algorithm," in *2016 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, 2016, pp. 313–315.
[29] K. N. Baharim, M. S. Kamaruddin, and F. Jusof, "Leveraging Missing Values in Call Detail Record Using Naïve Bayes for Fraud Analysis," in *2008 International Conference on Information Networking*, 2008, pp. 1–5.
[30] W. Xu and Y. Liu, "An Optimized SVM Model for Detection of Fraudulent Online Credit Card Transactions," in *2012 International Conference on Management of e-Commerce and e-Government*, 2012, pp. 14–17.
[31] J. L. L. Herrera, H. V. R. Figueroa, and E. J. R. Ramírez, "Deep fraud. A fraud intention recognition framework in public transport context using a deep-learning approach," in *2018 International Conference on Electronics, Communications and Computers (CONIELECOMP)*, 2018, pp. 118–125.
[32] Y. Wang *et al.*, "Privacy Preserving Distributed Deep Learning and Its Application in Credit Card Fraud Detection," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2018, pp. 1070–1078.
[33] Z. Kazemi and H. Zarrabi, "Using deep networks for fraud detection in the credit card transactions," in *2017 IEEE 4th International Conference on Knowledge-Based Engineering and Innovation (KBEI)*, 2017, pp. 0630–0633.
[34] E. M. Carneiro, L. A. V. Dias, A. M. d Cunha, and L. F. S. Mialaret, "Cluster Analysis and Artificial Neural Networks: A Case Study in Credit Card Fraud Detection," in *2015 12th International Conference on Information Technology - New Generations*, 2015, pp. 122–126.
[35] X. Min and R. Lin, "K-Means Algorithm: Fraud Detection Based on Signaling Data," in *2018 IEEE World Congress on Services (SERVICES)*, 2018, pp. 21–22.
[36] Y. Yu, X. Wan, G. Liu, H. Li, P. Li, and H. Lin, "A combinatorial clustering method for sequential fraud detection," in *2017 International Conference on Service Systems and Service Management*, 2017, pp. 1–6.
[37] W. Dong, W. Quan-yu, Z. Shou-yi, L. Feng-xia, and W. Da-zhen, "A feature extraction method for fraud detection in mobile communication networks," in *Fifth World Congress on Intelligent Control and Automation (IEEE Cat. No.04EX788)*, 2004, vol. 2, pp. 1853-1856 Vol.2.
[38] T. Fawcett and F. Provost, "Adaptive Fraud Detection," *Data Min. Knowl. Discov.*, vol. 1, no. 3, pp. 291–316, Sep. 1997.

[39] J.-S. Chang and W.-H. Chang, "An early fraud detection mechanism for online auctions based on phased modeling," presented at the 2009 Joint Conferences on Pervasive Computing, JCPC 2009, 2010, pp. 743–748.
[40] J.-S. Chang and W.-H. Chang, "Analysis of fraudulent behavior strategies in online auctions for detecting latent fraudsters," *Electron. Commer. Res. Appl.*, vol. 13, no. 2, pp. 79–97, Mar. 2014.
[41] C. Chiu, Y. Ku, T. Lie, and Y. Chen, "Internet Auction Fraud Detection Using Social Network Analysis and Classification Tree Approaches," *Int. J. Electron. Commer.*, vol. 15, pp. 123–147, Apr. 2011.
[42] P. Ferreira, R. Alves, O. Belo, and L. Cortesão, "Establishing Fraud Detection Patterns Based on Signatures," in *Advances in Data Mining. Applications in Medicine, Web Mining, Marketing, Image and Signal Mining*, 2006, pp. 526–538.
[43] R. J. Bolton, D. J. Hand, and D. J. H, "Unsupervised Profiling Methods for Fraud Detection," in *Proc. Credit Scoring and Credit Control VII*, 2001, pp. 5–7.
[44] C. Whitrow, D. J. Hand, P. Juszczak, D. Weston, and N. M. Adams, "Transaction aggregation as a strategy for credit card fraud detection," *Data Min. Knowl. Discov.*, vol. 18, no. 1, pp. 30–55, Feb. 2009.
[45] A. Correa Bahnsen, D. Aouada, A. Stojanovic, and B. Ottersten, "Feature engineering strategies for credit card fraud detection," *Expert Syst. Appl.*, vol. 51, pp. 134–142, Jun. 2016.
[46] S. Panigrahi, A. Kundu, S. Sural, and A. K. Majumdar, "Credit card fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning," *Inf. Fusion*, vol. 10, no. 4, pp. 354–363, Oct. 2009.
[47] A. Eshghi and M. Kargari, "Introducing a new method for the fusion of fraud evidence in banking transactions with regards to uncertainty," *Expert Syst. Appl.*, vol. 121, pp. 382–392, May 2019.