Volume 1, Issue 1, 2021

TECH-HNOWLEDGE JOURNAL

A Survey On Fraud Detection Techniques in E-Commerce

Suha M. Najem*, Suhad M. Kadeem
Department of Computer Science, University of Technology, Baghdad, Iraq
* cs.19.46@grad.uotechnology.edu.iq

Keywords: **E-Commerce, Fraud Detection Methods, Data Mining, Machine Learning, Hybrid Methods.**

ABSTRACT

Electronic commerce or e-commerce is a business model that lets companies and persons over the internet buy and sell anything. Recently, in the age of the Internet and forwarding to E-commerce, lots of data are stored and transferred from one location to another. Data that transferred can be exposed to danger by fraudsters. There is a massive increase in fraud which is leading to the loss of many billions of dollars worldwide every year. There are various modern ways of detecting fraud that is regularly proposed and applied to several business fields. The main task of Fraud detection is to observe the actions of tons of users to detect unwanted behavior. To detect these various kinds, data mining methods & machine learning to have been proposed and implemented to lessen down the attacks. A long time ago, many methods are utilized for fraud detection system such as Support Vector Machine (SVM), K-nearest Neighbor (KNN), neural networks (NN), Fuzzy Logic, Decision Trees, and many more. All these techniques have yielded decent results but still needing to improve the accuracy even further, by developing the techniques themselves or by using a hybrid learning approach for detecting frauds. In this paper, a review to describe the latest studies on fraud detection in e-commerce between (2018-2020), and a general analysis of the results- achieved and upcoming challenges for further researches. This will be useful for giving us complete visualization about how can we present the most suitable, most accurate methods for fraud detection in e-commerce transactions.

1.0. INTRODUCTION

E-commerce has expanded to make goods & products easier to detect and purchase through marketplaces and online retailers. Small businesses, independent freelancers, and large companies have all profited from e-commerce, which enables them to show their products and services widely that was not feasible with traditional offline retail.

With the growth of e-commerce, fraud has expanded seriously. “Fraud is nothing new to the merchant, since the beginning of time, man has always looked for the opportunity to defraud others — to gain goods or services without making payment.” [1].

In order to avert damages caused by fraud, dealers must implement strategies for fraud prevention and fraud detection. Sometimes there is confusion between fraud prevention & fraud detection. [2] make this distinction clear, “Fraud prevention describes measures to stop fraud from occurring in the first place (...) In contrast, fraud detection involves identifying fraud as quickly as possible once it has been perpetrated.” [3].

Fraud detection has been searched in several aspects with different approaches. Still, there is a huge volume of data, fraud detection by conventional methods becomes very hard. From here, the needing for techniques called “data mining”, based on statistical methods and artificial intelligence, is insistent[3].

In connection with the issue, data mining is used as exploratory data analysis with the assistance of other sciences in which searching for hidden and unknown information out of a huge amount of data is under focus. The operation of finding the hidden data or special information in a large amount of data is very hard and complicated. Merge of data mining with other methods such as machine learning, databases, and artificial intelligence has expanded very fast to detect patterns among such Data [4], [5], and [6].

This paper contains a review of fraud detection methods in e-commerce. The architecture of this paper shown as the second part describes how online payments work, the third part defines the fraud detection problem, the forth part define fraud detection methods, the fifth part list a review of precedent studies and the algorithms used in their researches, sixth part make discussion for the results of the related works and finally the conclusion about these studies.

2.0. E-COMMERCE: HOW ONLINE PAYMENTS WORK?

There are many ways for online customers to pay money to merchants, such as credit cards, direct debit, cash alternative payments, or mobile payments. However, credit card transactions still control the market of the e-commerce business [7]. Thus, it is important to understand how credit card payments work.

Figure 1 shows the stages of online credit card transactions. The first step the card number of the customer checked by the merchant to certain it is a legal card number (Card Authentication). Secondly, the merchant will request the bank who released the credit card to ensure that the credit card accounts not empty (Card Authorization). At last, the merchant requests the Settlement of the transaction, the physical transfer of the funds to the merchant’s bank. Figure 1 illustrates these steps [3]. If the customer pretended that he did not receive the service, product, or he became a victim of the fraudster, additional steps should take. In this case, the merchant can dispute the chargeback by providing documentation about the order. If the merchant cannot reverse the chargeback, he will have to return the money to the customer’s account and the sale is lost. Moreover, merchants can be subject to chargeback fees and fines from card associations if the chargeback rate is above their thresholds [7].

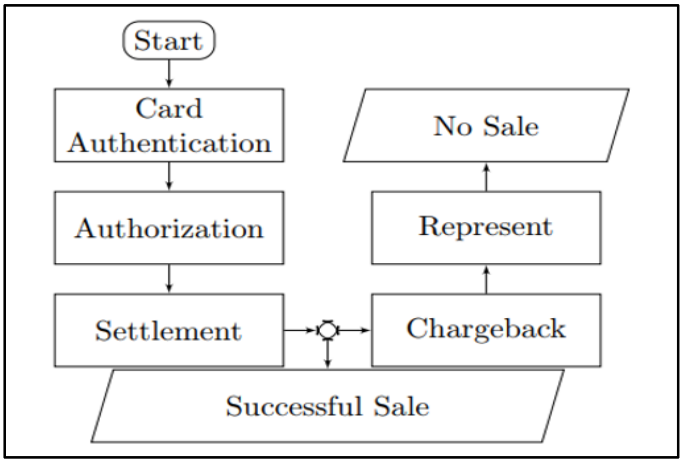

Fig. 1: Diagram of online payments steps. Source: [1]

3.0. THE FRAUD DETECTION PROBLEM

The most increased difficult data mining problem is fraud detection because fraudsters have the ability to change their behavior to look like legal behavior. This confusing behavior creates a serious challenge to differentiate between legitimate and fraud transactions. On the other hand, another difficulty with fraud detection is the imbalance between the number of fraud and legitimate transactions, fraud transactions always represent less than 1% of the entire transaction [2]. So, data analysts must make additional care with such imbalanced data sets.

4.0. Data analysis techniques for fraud detection

Fraud that involves credit card transactions, cell phones, tax return claims, insurance claims, government procurement, etc. represents serious problems for companies and businesses, so specialized analysis techniques are required for detecting fraud. These techniques belong to the space of Data Mining, Knowledge Discovery in Databases (KDD), Statistics, and Machine Learning. Techniques used for fraud detection fall into two primary classes: statistical techniques and artificial intelligence.

4.1. Hybrid Methods

The hybrid methods are come into being for particular types of problems. It is a mixing of more than two similar traditional methods to generate a more robust algorithm. Hybrid models can be implemented in several ways such as the lower level (preprocessing stage) technique and the highest-level technique. The output of the first phase is the input for the next phase[8]. The steps of the traditional algorithm may merge in the hybrid model to implement a completely new step or system[8]. Hybrid models are used for particular problem areas where the goal is to achieve better performance such as classification ability, computation efficiency, and ease of use. Data modification is first performed to classification concerning with the lower level (pre-processing step) technique[9]. Although many studies have been done using different methods and algorithms, many hybrid methods are typically used to provide better results and help to deal with the drawbacks of other methods. The continuously new attack is observed and so there is a need for advanced methods for detecting such frauds from the datasets. Hyperdization of various methods can be useful to detect fraud at an early stage [10].

5.0. RELATED WORKS

1. (Wang et al., 2018) They design "a deep auto-encoder" by using the similarity of vector representations. To recreate unique bipartite chart taxonomy and estimated that experimental comparability about user conduct. That profound embedding comes about Might after that be utilized for compelling fraud block identification by position circulation of client vector representations. DeepFD not just altogether outperforms other benchmark methods but will be likewise All the stronger for programmed identification of various duplicity obstructs.
2. (Xuan et al., 2018). This paper has examined the performance of two types of random forest models. The primary is the ordinary random forest, during every interior node, it haphazardly selects a subset of qualities Furthermore computes those focuses on different classes. The second algorithm is CART (Classification Also Regression Trees), during each node, it parts dataset Toward picking those best quality done a subset of qualities as stated by Gini impurity which measures vulnerability about the dataset. The first algorithm gives Accuracy (91.96%), Precision (90.27%), Recall (67.89%) and F-Measure (0.7811), while the second algorithm gives Accuracy (96.77%), Precision (89.46%), Recall (95.27%) and F-Measure (0.9601).

3. (Roy et al., 2018), evaluate the general artificial neural network (as a part of Deep Learning topologies) with built-in topologies like memory and time components such as Long Short-term memory – and changing parameters with respect to their effectiveness in fraud detection.
4. (Yee, Sagadevan and Malim, 2018), this paper using Bayesian network classifiers namely Tree Augmented Naïve Bayes (TAN), K2, logistics, J48, and Naïve Bayes classifiers which is all supervised based. All the classifiers give more than 95.0% accuracy when preprocessing the dataset using Principal Component Analysis and normalization, in contrast to scores obtained before preprocessing the dataset. In general, all the Bayesian classifiers give notably better scores after being fed with filtered data.
5. (Shakya, 2018). He uses a combination of different resampling techniques with Predictive models such as random forest, logistic regression, and XGBoost to prophesy if a transaction is legitimate or fraudulent. A hybrid resampling approach of Tomek Links removal and Synthetic Minority Over-Sampling Technique (SMOTE) with random forest algorithm giving best results coppered with other models.
6. (Saputra and Suharjito, 2019). This study processes the imbalances in the datasets of e-commerce fraud transaction by using the Synthetic Minority over Sampling Technique (SMOTE) and approved that the SMOT increasing the performance of data classification which is always unbalanced data, then use is the neural network, Naïve Bayes, random forest and decision tree. The results proved that the highest accuracy was for ANN with 96%, then RF and NB were 95%, for DT accuracy was 91.
7. (Zhang et al., 2019), their fraud detection system based on homogeneity-oriented behavior analysis (HOBA) which combines an advanced feature engineering process with a deep learning architecture. They approved the efficiency of their model by comparing it with other models like benchmark methods.
8. (Ramyashree et al., 2019). A “machine learning algorithm” produced as one of the standard models, which is used to detect fraud in e-commerce transactions. After that, add, “AdaBoost and majority vote method”, which is a hybrid method. In addition, this powerful algorithm can perform an evaluation of the noisy data samples. Good accuracy rates provided by "majority voting". 0.942 for 30% added noise is the score of several voting methods. Then, it was consummated that the voting method indicated a lot of stable execution in the presence of noise.
9. (Lucas et al., 2019). In this paper they benefit from the temporal data to produce " a strategy to quantify the covariate shift ", this strategy classifies the transactions in each day versus every other (that is there is a covariate shift between days when the classification is good and similar if the classification is not efficient. It is used as a distance matrix describing the covariate shift between days. Then applying the agglomerative clustering algorithm on it. Using a Random Forest classifier, they show that coordinating the information of the sort of the day previously recognized increments the Recall Precision- AUC by (2.5%).
10. (D.G et al., 2019). In this paper hybrid method called " CPNN-GA" proposed, which is consist of a combination of A genetic and artificial neural network algorithms for the detect anomaly in online transaction systems, where GA is an efficient algorithm for selecting optimal parameter so that optimize the quality of solution regarding classification with rate low false alarm rate and high fraud catching. Experiments show that the accuracy of CPPN is (84.42), GA (89.42) but CPPN-GA (95.58 9) with the highest hit rate (97.19).
11. (Benchaji, Douzi and El Ouahidi, 2019). In this study, the writers proposed an oversampling strategy by using K-Means clustering and genetic algorithm to increase the enhancement of

fraud detection in e-banking. This strategy used in imbalanced data set's minority class for data. The model contributed to the reduction of the number of false alerts and fraudulent transactions.

12. (Carta et al., 2019). The ensemble approach proposed in this paper can deal with some familiar problems that have an effect on classification problems by specifies this problem and the volume of risks so as to achieve higher precision in fraudulent transactions compared with other classification approaches. This model dealing with problems like data imbalance and increasing the number of frauds which detect correctly
13. (Yang et al., 2019) .they solve the problem of decreasing classification performance which comes from the noisy points in AdaBoost, resulting, via clustering algorithm. The strategy of this algorithm is to determine noisy points in the group of iterations. And in each iteration for every cluster, it computes a misclassification degree which is used to determine if a misclassified sample in the current iteration is a noisy point or not. Moreover, they produced an elastic approach for the misclassified samples to update the weights. Their method achieves better results than the state-of-the-art methods including LogitBoost, AdaBoost, AdaCoast, and SPLBoost.
14. 1(Varmedja et al., 2019). Their study was about comparison among some machine learning algorithms. Finally, the comparison confirmed that the Random Forest algorithm gives the best classification of whether transactions are fraud or not (RF with accuracy (99.96%), LR (97.46 %.) and NB (99.23%).
15. (Xie et al., 2019). They propose a novel approach of feature engineering for credit card fraud detection, by generate group features from individual behavior. The problem of temporal features exceeded effectively. Their method approved its effectiveness in improving the performance of fraud detection.
16. (Simi. M, 2019) they make comparisons among (Random Forest, SVM, and ANN) machine learning algorithms for credit card fraud detection. They conclude that is Random Forest has more accuracy than SVM and less accuracy than ANN in fraud detection.
17. (Sadgali, Sael and Benabbou, 2019). They reviewed the methods and techniques which showed superior results. And they found that hybrid fraud detection techniques are the most frequently used in fraud detection methods by determining the methods and techniques that give the best outcomes that have been idealized up until this point.
18. (Porwal and Mukund, 2019). They produce an ensemble of clustering methods in large data sets to detect fraudulent patterns by using a consistency score for each data point. Their method approved their power in outlier detection in large datasets and changing patterns.
19. (Devi, Biswas and Purkayastha, 2019)). In this work, a random forest algorithm has been developed with cost-sensitive weights to improve the effectiveness of credit card fraud detection. In the training phase and for each tree, a cost-function has been defined, more weight has been assigned for the minority instances during training. The trees are arranged as stated by their ability prediction of the minority class instances. The model has not been checked for high-dimensional datasets. The performance of the proposed method is (F-measure [76.815], G-mean [82.298], and AUC [0.778].
20. (Makki et al., 2019). In this paper, they make a comparison among eight machine learning algorithms performance, and the class imbalance problem has been solved by some solutions. They studied the weakness and the performance of approaches applied to credit card fraud detection. They found that the LR, C5.0 decision tree algorithm, SVM, and ANN are the best methods according to the 3 considered performance measures (Accuracy, Sensitivity, and AUPRC).

21. (Shirgave et al., 2019). Various machine learning algorithm has been reviewed for fraud detection in credit card transaction with the performance based on precision, accuracy, and specificity metrics. The alert has been checked as fraudulent or authorized by using the Random Forest classifier. By using delayed and feedback supervised sample. The classifier will be trained, which gives an accuracy (0.962), Precision (0.997), and Specificity (0.987).
22. (Nakai, 2020) . He developed the fraud detection model without a supervised label based on anomaly detection and succeeded in detecting certified fraud contracts in the top rank. He solved the problem of the impossibility to detect fraud in the supervised label when the number of fraudulent transactions is extremely few.
23. (Lucas et al., 2020).in this paper a feature engineering strategy has been Adopted by HMM, which permits us to integrate consecutive knowledge in the transactions in the form of HMM-based features. These features which based on HMM- have the ability to make a Random Forest classifier (non-sequential classifier) to use sequential information for the classification process. The strategy of the automated feature engineering based on HMM has "multiple perspective property" which enables us to benefit from incorporating a wide range of sequential information. Actually, the study differentiates the genuine from fraudulent behaviors of the card-holders & the merchants with respect to timing and amount features of the transactions.
24. (Alazizi et al., 2020), they produce a new fraud detection technique called "DuSVAE model". The model is a combination of two" sequential variational auto-encoders" used in the input sequential data to construct a concentrated representation vector which then used as input to the classifier to give it the possibility of classification transactions as genuine or fraudulent.
25. (Mehana and Nuci, 2020)"An incremental learning approach "has been introduced as a new method for real-time fraud detection in online banking transactions. The model AFDM is analyzing transactions based on the transaction instead of accounts which gives more detailed information and represents a good assistant next to detection actions. In addition, the knowledge of the classification algorithm like NB can increment its Updatable transaction by transaction. This novel approach makes the detection and response possibility in real-time, and it gives accuracy (97,2). It also allowed learning new concepts of behavior changes immediately.
26. (Meng, Zhou and Liu, 2020).the fraudulent credit card transactions have been detected by using a hybrid method consists of an XGBoost algorithm preceded with a SMOTE algorithm which is in turn use to achieve the balance of data. The data balancing, make the model more generalized and stable.
27. (Alghofaili, Albattah and Rassam, 2020). They use the "Long Short-Term Memory (LSTM) technique" to improve the traditional financial fraud detection systems. The model identifies unknown and sophisticated patterns of fraud quickly and with high accuracy (99.95% in less than a minute) on a real dataset.
28. (Chen et al., 2019). In this work, they present a fraud detection system based on a graph- for large-scale e-commerce insurance with the cases of the most popular insurance - the security deposit insurance and the return-freight insurance". They also identify the modules and their functionality in this system. The - graphs and their learning algorithms contribute discover organized fraudsters and the model has helped save millions of dollars per year.
29. In (Daliri, 2020) a hybrid system based on the Artificial Neural Network (ANN) technique and Harmony Search Algorithm (HSA) is used to detect fraud. The parameters of ANN have been optimized by using HSA, and ANN is used to detect fraud. The system show accuracy with (86) and recall criteria (87).

30. In (Harwani et al., 2020), A hybrid approach consists of " Machine learning and Deep learning" presents for fraud detection, such methodologies can easily work on large datasets. Self-Organizing Maps [SOM] firstly used to detect potential frauds as an unsupervised learning approach and then applying Artificial Neural Network [ANN] as a supervised learning approach.
31. (S et al., 2020).They build the model using some supervised machine learning algorithms such as logistic regression, decision tree, support vector machine. In this project they used two features (time and amount) fundamentally for predicting if the transaction is fraud or not, the number of parameters of feature has been reduced by" time series analysis", then they use either average method, moving average, or window, the naive method and sessional naïve method for achieving the model but all these methods have some advantages and disadvantages.
32. (Tingfei, Guangquan and Kuihua, 2020). An "oversampling method based on the VAE" has been proposed as a new approach for fraud credit card detection. This approach is a new supervised oversampling method that can deal with the class imbalance of the datasets, but it is impossible to apply to unsupervised systems. Compared with SMOTE and GAN it shows less performance in recall metric and when the model deals with novel fraud data could perform badly.
33. (Babu et al., 2020). Evaluate the performance of "deliver regression, call tree and random woodland" to detecting the fraud in grasp card. Depending on the results, finding that selecting a random forest algorithm over XGboost can be a reasonable method to get the next degree of Inclusiveness with a little decrease in performance.
34. (B, Safont and Vergara, 2020). . They present a novel approach to increase fraud detection performance by using "the differences in temporal dependence (sequential patterns)" between valid and non-legitimate credit card operations. It is assumed that in feature spaces with low-dimension, the successive patterns are more notable than the features with high-dimension space of all of the card operation records. Linear and quadratic discriminant analyses, classification tree, and naive Bayes are the single classifiers used in this model. With these single classifiers and to get better results, Alpha integration has been applied.
35. (Zheng et al., 2020). An improvement is proposed to the TrAdaBoost algorithm (ITrAdaBoost) by changes the weight of the instance which is wrongly classified in a source scope, and then calculate the distance depending on the theory of" reproducing kernel Hilbert space". In addition, the concept drift problem in the transactions has been solved by applying the ITrAdaBoost algorithm. Unfortunately, the computation time is high because of the distribution distances.
36. (Taha and Malebary, 2020). An "optimized light gradient boosting machine (OLightGBM)" has been Proposed as an intelligent method of credit card detection. experimental results indicate that the proposed approach exceeded the other machine learning algorithms including (RF, LR, R-SVM, linear -SVM, KNN, DT, and NB) and achieved the highest performance in terms of Accuracy (98.40%), AUC (92.88%), Precision (97.34%) and F1-score (56.95%).
37. (Mittal, 2020). They propose an efficient learning strategy to determine the challenges (classification problem and performance measures) including "verification latency and audio feedback communication". This learning strategy applied to a wide range of credit card transactions.
38. (Zhang et al., 2020) A new method proposed for solving the problem of" low-frequency users with small transaction amount", the current approaches cannot exactly illustrate transaction behavior for such users. Besides, it tacks in consideration the" current trading group behavior

and current transaction status", and draw a new behavior for low-frequency user. To detect the user’s current transaction, they produce an approach based on" user behavior and Naive Bayes".

39. (Jagdish, Singh and Yadav, 2020). They proposed "MFDA (Modified Fisher Discriminant Analysis)"for fraud credit card detection. The study solves the shortcoming in FDM, the generated results were not accurate when using input values with little less sensitivity. In addition to MFDA, several algorithms are used (DT, ANN, NB, and Normal Fisher). Experiments show that FDMA has the highest accuracy.
40. (Trivedi et al., 2020). A feedback system mechanism based on machine learning methodology has been introduced as efficient fraud detection for a credit card. This method improves the rate of classifier detection aside from cost-effectiveness. The experiments show that random forest techniques show an accuracy percentage of 95.988 %, although SVM 93.228 %, LR 92.89 %, NB 91.2 %, Decision trees 90.9 %.
41. (Priscilla and Prabha, 2020)Their research is a review on Credit Card Fraud Detection (CCFD), the problem of class imbalance in datasets and Machine Learning approaches. The conclusion of the review is Supervised Learning is highly used than the unsupervised for CCFD, the fraud detection techniques which are most commonly used are SVM, Bayesian classifiers, LR, and DT, and Random Forest is the most usage frequency Ensemble learning technique with a good performance. finally, Hybrid methods are better than using a single classifier.
42. (Li et al., 2021). They improve the support vector machine parameters by using a cuckoo search algorithm to raise the ability to detect fraud of credit cards. The results demonstrate that CS-SVM is superior to SVM in Accuracy, Precision, Recall, F1-score, AUC, and superior to LR, RF, DT, and NB, whose accuracy is 98%.

6.0. DISCUSSION

Many metrics used for evaluating the result of fraud detection systems such as (Precision, Accuracy, Recall….), so that different methods give different evaluation depending on the method or methods used in the system.

There are many techniques in machine learning (supervised, unsupervised, ensemble, and deep learning). Table.2 (V. Priscilla and P. Prabha.2020) shows that most fraud detection systems use supervised learning and the most supervised learning methods frequency usage is relatively convergent (Bayesian network, logistic regression, decision tree, and support vector machine) but the ensemble technique (random forest) is the best performance and most frequency usage among other techniques .farther more, many studies show that the hybrid methods give higher performance than using one method and using search algorithms to optimize parameters of classification algorithms give the best results. Table .3 show the data sets used in most studies with their instance numbers. (V. Priscilla and P. Prabha.2020) [18, 37, 74, 75].

Table 2. Usage frequency of machine learning techniques in CCFD

Machine learning	*Methods*	*Accuracy*	*Precision*	*Recall*	*usage frequency*	*References*	*advantages*	*disadvantages*
Supervised Learning	*Neural Network*	*98.69*	*98.41*	*98.98*	*17*	*[4,17,19,20,32,36,38,52,53,54,55,56,57,72,75,78,82]*	*Highly accurate and reliable*	*Need to understand and label the input* *More computation time required for the training phase*
	Support Vector Machine	*93.96*	*93.22*	*93.00*	*20*	*[21,33,38,39,53,59,61,62,63,64,65,66,67,68,69,70,71,74,75,78]*		
	Bayesian Network Classifiers	*91.62*	*97.09*	*84.82*	*21*	*[20,21,35,39,42,47,55,56,58,59,61,64,66,67,73,74,78,80,82,87,93]*		
	K-Nearest Neighbor	*94.99*	*94.58*	*92.00*	*6*	*[39,64,67,73,81,82]*		
	Logistic Regression	*94.84*	*97.58*	*92.00*	*21*	*[21,33,36,39,42,52,53,55,59,61,63,64,66,71,73,74,75,82,83,84,85]*		
	Decision Tree	*92.88*	*99.48*	*86.34*	*21*	*[20,21,33,35,39,51,52,53,55,59,63,64,66,69,73,74,75,82,83,84,85]*		
Unsupervised Learning	*Expectation-Maximization*				*1*	*[58]*	*Easy to find unknown patterns and features of data*	*Computationally complex* *Less accurate due to unlabeled input*
	K-Means				*3*	*[14,58,64]*		
	FuzzyC-Means				*1*	*[57]*		
	DBSCAN				*1*	*[55]*		
	Hidden Markov Model (HMM)				*4*	*[23,55,56,89]*		
	Self-Organizing Map (SOM)				*1*	*[55]*		
	LINGO				*1*	*[90]*		

Ensemble Learning	*Random Forest*	*99.96*	*96.38*	*81.63*	*32*	*[13,18,21,22,23,35,36,37,38,39,42,45,51,52,53,54,59,61,63,65,66,67,69,71,72,78,81,82,84,85,91,93]*	*Avoid the overfitting problem and gives better predictions when compared with a single model*	*Computation time is high Reduces model interpretability due to increased complexity*
	Boosting				*7*	*[53,65,69,70,71,82,92]*		
	Bagging				*3*	*[64,93,64]*		
	Voting				*1*	*[93]*		
Deep Learning	*Stochastic Gradient Descent*				*1*	*[82]*	*No need for feature extraction and labeling of data*	*A large amount of data is needed to find the pattern Create overfitting problem in the model*
	Long short-term memory				*4*	*[32,26,61, 91]*		
	Deep Feed Forward NN				*3*	*[83,92,95]*		
	Variational Autoencoder (VAE)				*3*	*[10,40,95]*		
	Auto Encoder (AE)				*2*	*[68,54]*		
	Restricted Boltzmann Machines				*1*	*[54]*		
	Recurrent Neural Network				*2*	*[32,61]*		
	Convolutional Neural Network				*1*	*[54]*		
	Generative Adversarial Network				*1*	*[98]*		

Table 3: Dataset used for CCFD.

Dataset	*N0.of instances*	*Fraud instances*	*References*	*source*
UCSD-FICO Data Mining Contest 2009	*100,000*	*2293*	*[59,64,67,80, 94]*	*https://www.cs.purdue.edu/commugrate/data/credit_card/*
European – Credit card transaction	*284.807*	*492*	*[11,,13,21,27,29,36,40, 41,42,51,65,73,74,82,85 ,95,97,98,]*	*https://www.kaggle.com/mlg-ulb/creditcardfraud*
German– Credit	*1000*	*300*	*[4,18,82,84,93,97,99]*	*UCI Machine learning repository*
Taiwan– Default Credit Card	*30000*	*6636*	*[53]*	*https://www.kaggle.com/uciml/default-of-credit-card-clients-dataset*
Australian-Credit Approval	*690*	*307*	*[18, 70 ,97]*	*https://data.world/uci/credit-approval*
cc Fraud	*1048575*	*62739*	*[100]*	*https://packages.revolutionanalytics.com/datasets/*
Belgian credit cards	*10000*		*[22]*	
e-commerce company of China	*30,000,000*	*82,000*	*[78]*	
Confidential data from bank			*[12,20,32,48,52,54,63,65,66,69,72,81,83, 87, 92,94, 101,76]*	
Synthetic data			*[25,43,56,57,88]*	
Simulated data			*[47,55,58 ,90]*	
Amazon Instrument and Amazon Movie			*[43]*	

7.0. CONCLUSION

This survey, display fraud detection methods in fraud detection systems depending on studies of the latest three years, which include a combination of data mining techniques and artificial intelligence. Many algorithms and different metrics used to evaluate the results, but in general Random Forest has the highest frequency usage, and experiments show that its methodology is most accurate (although it is not used in 2020), followed by Logistic Regression and Support Vector Machines. Decision trees are easy to understand and implement, so DT models good in (classification, regression, and feature selection). Hybrid methods give the best accuracy than using the individual method. Naive Bayes algorithms are easy to implement in engineering and easy to work in fraud detection models, but NB classifier is a log-linear model, subsequently, it is not optimal for non-linear problems with high complexity. Adding approaches like AdaBoost or decision trees can solve the non-linear problems and the weakness in learning machines.

REFERENCES

[1] David Montague (no date) Essentials of Online Payment Security and Fraud Prevention. Edited by I. John Wiley & Sons. doi: 10.1002/9781118386750.

[2] Bolton, R. J. et al. (2002) 'Statistical Fraud Detection: A ReviewCommentCommentRejoinder', Statistical Science, 17(3), pp. 235–255. doi: 10.1214/ss/1042727940.

[3] Carneiro, N. A. (2016) 'A data mining approach to fraud detection in e-tail: A case study in an online luxury fashion retailer', (January). Available at: https://repositorio-aberto.up.pt/bitstream/10216/95618/2/117705.pdf.

[4] Daliri, S. (2020) ‘Using Harmony Search Algorithm in Neural Networks to Improve Fraud Detection in Banking System’, Computational Intelligence and Neuroscience, 2020. doi: 10.1155/2020/6503459.
Sithic, H. L. and Balasubramanian, T. (2013) ‘Survey of Insurance Fraud Detection Using Data Mining Techniques’, (3), pp. 62–65.
[5] Padhy, N., Mishra, P. and Panigrahi, R. (2012) ‘The Survey of Data Mining Applications and Feature Scope’, (June 2017). doi: 10.5121/ijcseit.2012.2303.
[6] Lim, W. et al. (2016) ‘Conditional Weighted Transaction Aggregation for Credit Card Fraud Detection to cite this version: HAL Id: hal-01393754’.
[7] Duman, E. and Ozcelik, M. H. (2011) ‘Detecting credit card fraud by genetic algorithm and scatter search’, Expert Systems with Applications, 38(10), pp. 13057–13063.
[8] Jans, M. et al. (2011) ‘A business process mining application for internal transaction fraud mitigation’, Expert Systems with Applications, 38(10), pp. 13351–13359.
[10] Alazizi, A. et al. (2020) ‘Dual Sequential Variational Autoencoders for Fraud Detection’, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 12080 LNCS, pp. 14–26. doi: 10.1007/978-3-030-44584-3_2.
[11] Alghofaili, Y., Albattah, A. and Rassam, M. A. (2020) ‘A Financial Fraud Detection Model Based on LSTM Deep Learning Technique’, Journal of Applied Security Research, 0(0), pp. 1–19. doi: 10.1080/19361610.2020.1815491.
[12] B, A. S., Safont, G. and Vergara, L. (2020) ‘from Credit Card Operations’, pp. 287–296.
[13] Babu, M. G. et al. (2020) ‘A Machine Learning Approach for Credit Card Fraud Detection’, (5237), pp. 5237–5244.
[14] Benchaji, I., Douzi, S. and El Ouahidi, B. (2019) Using genetic algorithm to improve classification of imbalanced datasets for credit card fraud detection, Lecture Notes in Networks and Systems. Springer International Publishing. doi: 10.1007/978-3-030-11914-0_24.
[15] Reena G.Bhati "A Review on Present Technologies for Fraud Detection Using Data Mining ", Computer Science Department, TMV, PUNE, INDIA, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 7, 2019 (Special Issue) © Research India Publications. http://www.ripublication.com.Carta, S. et al. (2019) ‘Fraud detection for E-commerce transactions by employing a prudential Multiple Consensus model’, Journal of Information Security and Applications, 46(February), pp. 13–22. doi: 10.1016/j.jisa.2019.02.007.
[16] Chen, C. et al. (2019) ‘InfDetect: A Large Scale Graph-based Fraud Detection System for E-Commerce Insurance’, Proceedings - 2019 IEEE International Conference on Big Data, Big Data 2019, (March), pp. 1765–1773. doi: 10.1109/BigData47090.2019.9006115.
[17] D.G, A. et al. (2019) ‘Hybrid Design using Counter Propagation Neural Network-Genetic Algorithm Model for the Anomaly Detection in Online Transaction’, International Journal of Advances in Scientific Research and Engineering, 5(9), pp. 107–114. doi: 10.31695/ijasre.2019.33512.
[18] Devi, D., Biswas, S. K. and Purkayastha, B. (2019) ‘A Cost-sensitive weighted Random Forest Technique for Credit Card Fraud Detection’, 2019 10th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2019, (July). doi: 10.1109/ICCCNT45670.2019.8944885.
[19] Harwani, H. et al. (2020) ‘Credit Card Fraud Detection Technique using Hybrid Approach: An Amalgamation of Self Organizing Maps and Neural Networks’, International Research Journal of Engineering and Technology. Available at: www.irjet.net.
[20] Jagdish, S., Singh, M. and Yadav, V. (2020) ‘Credit Card Fraud Detection System: A Survey’, Journal of Xidian University, 14(5). doi: 10.37896/jxu14.5/599.
[21] Li, C. et al. (2021) ‘Application of Credit Card Fraud Detection Based on CS - SVM’, 11(1). doi: 10.18178/ijmlc.2021.11.1.1011.
[22] Lucas, Y. et al. (2019) ‘Dataset shift quantification for credit card fraud detection’, Proceedings - IEEE 2nd International Conference on Artificial Intelligence and Knowledge Engineering, AIKE 2019, (June), pp. 97–100. doi: 10.1109/AIKE.2019.00024.
[23] Lucas, Y. et al. (2020) ‘Towards automated feature engineering for credit card fraud detection using multi-perspective HMMs’, Future Generation Computer Systems, 102, pp. 393–402. doi: 10.1016/j.future.2019.08.029.
[24] Makki, S. et al. (2019) ‘An Experimental Study With Imbalanced Classification Approaches for Credit Card Fraud Detection’, IEEE Access, 7, pp. 93010–93022. doi: 10.1109/ACCESS.2019.2927266.
[25] Mehana, A. and Nuci, K. P. (2020) ‘Fraud Detection using Data-Driven approach’, pp. 1–7. Available at: http://arxiv.org/abs/2009.06365.
[26] Meng, C., Zhou, L. and Liu, B. (2020) ‘A case study in credit fraud detection with SMOTE and XGboost’, Journal of Physics: Conference Series, 1601(5). doi: 10.1088/1742-6596/1601/5/052016.

[27] Mittal, P. (2020) '[CREDIT CARD FRAUD DETECTION SYSTEM]', (May), pp. 0–27. doi: 10.13140/RG.2.2.28192.81924.

[28] Nakai, M. (2020) 'Fraud Detection without Label', (January). School of Industrial Technology, Advanced Institute of Industrial Technology.

[29] Porwal, U. and Mukund, S. (2019) 'Credit card fraud detection in E-commerce', Proceedings - 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering, TrustCom/BigDataSE 2019. doi: 10.1109/TrustCom/BigDataSE.2019.00045.

[30] Priscilla, C. V. and Prabha, D. P. (2020) 'Credit Card Fraud Detection: A Systematic Review', 1, pp. 290–303. doi: 10.1007/978-3-030-38501-9_29.

[31] Ramyashree, K. et al. (2019) 'A hybrid method for credit card fraud detection using machine learning algorithm', International Journal of Recent Technology and Engineering, 7(6), pp. 235–239.

[32] Roy, A. et al. (2018) 'Deep learning detecting fraud in credit card transactions', 2018 Systems and Information Engineering Design Symposium, SIEDS 2018, pp. 129–134. doi: 10.1109/SIEDS.2018.8374722.

[33] S, V. K. K. et al. (2020) 'Credit Card Fraud Detection using Machine Learning Algorithms', 9(07), pp. 1526–1530.

[34] Sadgali, I., Sael, N. and Benabbou, F. (2019) 'Performance of machine learning techniques in the detection of financial frauds', in Procedia Computer Science. Elsevier B.V., pp. 45–54. doi: 10.1016/j.procs.2019.01.007.

[35] Saputra, A. and Suharjito (2019) 'Fraud detection using machine learning in e-commerce', International Journal of Advanced Computer Science and Applications, 10(9).

[36] Shakya, R. (2018) 'Application of Machine Learning Techniques in Credit Card Fraud Detection', (December), pp. 1–67.

[37] Shirgave, S. K. et al. (2019) 'A Review On Credit Card Fraud Detection Using Machine Learning', (October).

[38] Simi. M. J. (2019) 'Credit Card Fraud Detection: A Comparison using Random Forest, SVM and ANN', International Research Journal of Engineering and Technology, 225. Available at: www.irjet.net.

[39] Taha, A. A. and Malebary, S. J. (2020) 'An Intelligent Approach to Credit Card Fraud Detection Using an Optimized Light Gradient Boosting Machine', IEEE Access, 8, pp. 25579–25587. doi: 10.1109/ACCESS.2020.2971354.

[40] Tingfei, H., Guangquan, C. and Kuihua, H. (2020) 'Using Variational Auto Encoding in Credit Card Fraud Detection', IEEE Access, 8, pp. 149841–149853. doi: 10.1109/ACCESS.2020.3015600.

[41] Trivedi, N. K. et al. (2020) 'An efficient credit card fraud detection model based on machine learning methods', International Journal of Advanced Science and Technology, 29(5), pp. 3414–3424.

[42] Varmedja, D. et al. (2019) 'Credit Card Fraud Detection - Machine Learning methods', 2019 18th International Symposium INFOTEH-JAHORINA, INFOTEH 2019 - Proceedings, (October), pp. 1–5. doi: 10.1109/INFOTEH.2019.8717766.

[43] Wang, H. et al. (2018) 'Deep Structure Learning for Fraud Detection', Proceedings - IEEE International Conference on Data Mining, ICDM, 2018-Novem(November), pp. 567–576. doi: 10.1109/ICDM.2018.00072.

[44] Xie, Y. et al. (2019) 'A Feature Extraction Method for Credit Card Fraud Detection', Proceedings - 2019 2nd International Conference on Intelligent Autonomous Systems, ICoIAS 2019, (February), pp. 70–75. doi: 10.1109/ICoIAS.2019.00019.

[45] Xuan, S. et al. (2018) 'Random forest for credit card fraud detection', ICNSC 2018 - 15th IEEE International Conference on Networking, Sensing and Control, pp. 1–6. doi: 10.1109/ICNSC.2018.8361343.

[46] Yang et al. (2019) 'AClustring-based Flexible Weighting Methodin AdaBoost andits Application to Transaction fraud detection'.

[47] Yee, O. S., Sagadevan, S. and Malim, N. H. A. H. (2018) 'Credit card fraud detection using machine learning as data mining technique', Journal of Telecommunication, Electronic and Computer Engineering, 10(1–4), pp. 23–27.

[48] Zhang, X. et al. (2019) 'HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture', Information Sciences, (May). doi: 10.1016/j.ins.2019.05.023.

[49] Zhang, Z. et al. (2020) 'A Fraud Detection Method for Low-Frequency Transaction', IEEE Access, 8, pp. 25210–25220. doi: 10.1109/ACCESS.2020.2970614.

[50] Zheng, L. et al. (2020) 'Improved TrAdaBoost and Its Application to Transaction Fraud Detection', IEEE Transactions on Computational Social Systems, pp. 1–13. doi: 10.1109/tcss.2020.3017013.

[51] Wang, H., Zhu, P., Zou, X., Qin, S.: "An ensemble learning framework for credit card fraud detection based on training set partitioning and clustering". In: IEEE SmartWorld, Ubiquitous Intelligence and Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People and Smart City Innovations, SmartWorld/UIC/ATC/ScalCom/CBDCom/IoP/SCI 2018, pp. 94–98 (2018)

[52] Van Vlasselaer, V., et al.: APATE: a novel approach for automated credit card transaction fraud detection using network-based extensions. Decis. Support Syst. 75, 38–48 (2015)
[53] Akosa, J.: Predictive accuracy: a misleading performance measure for highly imbalanced data. In: Proceedings of the SAS Global Forum (2017)
[54] Fu, K., Cheng, D., Tu, Y., Zhang, L.: Credit card fraud detection using convolutional neural networks. In: Hirose, A., Ozawa, S., Doya, K., Ikeda, K., Lee, M., Liu, D. (eds.) Neural Information Processing, pp. 483–490. Springer, Cham (2016)
[55] Dai, Y., Yan, J., Tang, X., Zhao, H., Guo, M.: Online credit card fraud detection: a hybrid framework with big data technologies. In: Proceedings of 15th IEEE International Conference Trust Security and Privacy in Computing and Communication, 10th IEEE International Conference Big Data Science and Engineering, 14th IEEE International Symposium Parallel Distributed Processing, pp. 1644–1651 (2016)
[56] Batani, J.: An adaptive and real-time fraud detection algorithm in online transactions. Int. J. Comput. Sci. Bus. Inform. 17, 1–12 (2017)
[57] Behera, T.K., Panigrahi, S.: Credit card fraud detection: a hybrid approach using fuzzy clustering & neural network. In: Proceedings of 2015 2nd IEEE International Conference on Advances in Computing and Communication Engineering, ICACCE 2015, pp. 494–499 (2015)
[58] Santos, L.J.S., Ocampo, S.R.: "Bayesian method with clustering algorithm for credit card transaction fraud detection". Rom. Stat. Rev. 1, 103–120 (2018)
[59] Hassan, D.: The impact of false negative cost on the performance of cost sensitive learning based on Bayes minimum risk: a case study in detecting fraudulent transactions. Int. J. Intell. Syst. Appl. 9(2), 18–24 (2017)
[60] V. Mareeswari and G. Gunasekaran, "Prevention of credit card fraud detection based on HSVM," in IEEE International Conference on Information Communication and Embedded Systems, 2016.
[61] Wang, S., Liu, C., Gao, X., Qu, H., Xu, W.: Session-based fraud detection in online e-commerce transactions using recurrent neural networks. In: Altun, Y., et al. (eds.) Machine Learning and Knowledge Discovery in Databases. Lecture Notes in Computer Science, pp. 241–252. Springer, Cham (2017)
[62] Wang, C., Han, D.: Credit card fraud forecasting model based on clustering analysis and integrated support vector machine. Cluster Comput. 0123456789, 1–6 (2018)
[63] Carneiro, N., Figueira, G., Costa, M.: A data mining based system for credit-card fraud detection in e-tail. Decis. Support Syst. 95, 91–101 (2017)
[64] Zareapoor, M., Shamsolmoali, P.:" Application of credit card fraud detection: based on bagging ensemble classifier". Procedia Comput. Sci. 48(C), 679–685 (2015)
[65] Zhang, Y., Liu, G., Zheng, L., Yan, C., Jiang, C.: A novel method of processing class imbalance and its application in transaction fraud detection. In: 2018 IEEE/ACM 5th International Conference on Big Data Computing Applications and Technologies, vol. 1, pp. 152–159 (2018)
[66] de Sá, A.G.C., Pereira, A.C.M., Pappa, G.L.: A customized classification algorithm for credit card fraud detection. Eng. Appl. Artif. Intell. 72, 21–29 (2018)
[67] Seeja, K.R., Zareapoor, M.: FraudMiner: a novel credit card fraud detection model based on frequent itemset mining. Sci. World J. 2014, 1–10 (2014)
[68] Tran, P.H., Tran, K.P., Huong, T.T., Heuchenne, C., HienTran, P., Le, T.M.H.: Real time data-driven approaches for credit card fraud detection, pp. 6–9 (2018)
[69] Su, C.-H., et al.: A ensemble machine learning based system for merchant credit risk detection in merchant MCC misuse. J. Data Sci. 17(1) (2019)
[70] Niimi, A.:" Deep learning for credit card data analysis". In: 2015 World Congress on Internet Security (WorldCIS), pp. 73–77 (2015)
[71] Salo, F., Injadat, M., Nassif, A.B., Shami, A., Essex, A." Data mining techniques in intrusion detection systems: a systematic literature review". IEEE Access 6, 56046–56058 (2018)
[72] Dal pozzlo A., Caelen, O., Le Borgne, Y.A., Waterschoot, S., Bontempi, G.: Learned lessons in credit card fraud detection from a practitioner perspective. Expert Syst. Appl. 41 (10), 4915–4928 (2014)
[73] Awoyemi, J.O., Adetunmbi, A.O., Oluwadare, S.A.: Credit card fraud detection using machine learning techniques: a comparative analysis. In: Proceedings IEEE International Conference Computing Networking Informatics, ICCNI 2017, January 2017, pp. 1–9 (2017)
[74] N.K. Trivedi , S. Simaiya , U. K. Lilhore , S. K. Sharma ." An Efficient Credit Card Fraud Detection Model Based on Machine Learning Methods" . International Journal of Advanced Science and Technology Vol. 29, No. 5, (2020), pp. 3414 – 3424ز ISSN: 2005-4238 IJAST 3414 Copyright ⓒ 2020 SERSC

[75] S. MAKKI , Z. ASSAGHIR , Y. TAHER , R HAQUE , M.-S. HACID , H. ZEINEDDINE. " An Experimental Study with Imbalanced Classification Approaches for Credit Card Fraud Detection". Citation information: DOI 10.1109/ACCESS.2019.2927266, IEEE Access

[76] Zhang, Y., Liu, G., Luan, W., Yan, C., Jiang, C.: Application of SIRUS in credit card fraud detection. In: International Conference on Computational Social Networks, pp. 66–78 (2018)

[77] W. Lim, A. Sachan, V. Thing. 2014. "Conditional Weighted Transaction Aggregation for Credit Card Fraud Detection". HAL ID: hal-01393754

[78] S.Xuan, G. Liu, Z. Li, L. Zheng, S. Wang, C. Jiang. "Random Forest for Credit Card Fraud Detection". 978–1–5386–5053–0/18/$31.00 © 2018 IEEE.

[79] C. Li, N.Ding, H. Dong, and Y. Zhai ." Application of Credit Card Fraud Detection Based on CS-SVM". International Journal of Machine Learning and Computing, Vol. 11, No. 1, January 2021.

[80] Nur-E-Arefin, M., Islam, M.S.: Application of computational intelligence to identify credit card fraud. In: 2018 International Conference on Innovation in Engineering and Technology, ICIET 2018, pp. 1–6 (2018)

[81] Nami, S., Shajari, M.: Cost-sensitive payment card fraud detection based on dynamic random forest and k-nearest neighbors. Expert Syst. Appl. 110, 381–392 (2018)

[82] Saia, R., Carta, S.: Evaluating the benefits of using proactive transformed-domain-based techniques in fraud detection tasks. Future Gener. Comput. Syst. 93, 18–32 (2019)

[83] Kim, E., et al.: Champion-challenger analysis for credit card fraud detection: hybrid ensemble and deep learning. Expert Syst. Appl. 128, 214–224 (2019)

[84] Patil, S., Nemade, V., Soni, P.K.: Predictive modelling for credit card fraud detection using data analytics. Procedia Comput. Sci. 132, 385–395 (2018)

[85] Lakshmi, S., Kavila, S.D.: Machine learning for credit card fraud detection system. Int. J. Appl. Eng. Res. 13(24), 16819–16824 (2018)

[86] P. Save, P. Tiwarekar, N. Ketan and N. Mahyav anshi,"A Novel Idea for Credit Card Fraud Detection using Decision Tree," International Journal of Computer Applications,vol. 161, no. 13, pp. 6-9, 2017.

[87] Noghani, F.F., Moattar, M.-H.: Ensemble classification and extended feature selection for credit card fraud detection. J. AI Data Min. 5(2), 235–243 (2017)

[88] Artikis, A., et al.: A prototype for credit card fraud management: industry paper. In:Proceedings of the 11th ACM International Conference on Distributed and Event-Based Systems, pp. 249–260 (2017)

[89] Prakash, A., Chandrasekar . "An optimized multiple semi-hidden Markov model for credit card fraud detection". Indian J. Sci. Technol. 8(2), 176–182 (2015)

[90] Hegazy, M., Madian, A., Ragaie, M.: Enhanced fraud miner: credit card fraud detection using clustering data mining techniques. Egypt. Comput. Sci. 40(03), 72–81 (2016)

[91] Jurgovsky, J., et al.: Sequence classification for credit-card fraud detection. Expert Syst. Appl. 100, 234–245 (2018)

[92] Rushin, G., Stancil, C., Sun, M., Adams, S., Beling, P.: Horse race analysis in credit card fraud—deep learning, logistic regression, and Gradient Boosted Tree. In: 2017 Systems and Information Engineering Design Symposium (SIEDS), pp. 117–121 (2017)

[93] Kumari, P., Mishra, S.P.: Analysis of credit card fraud detection using fusion classifiers. In:Behera, H., Nayak, J., Naik, B., Abraham, A. (eds.) Computational Intelligence in Data Mining, vol. 711, pp. 111–122. Springer, Singapore (2019)

[94] Akila, S., Srinivasulu Reddy, U.: Cost-sensitive Risk Induced Bayesian Inference Bagging (RIBIB) for credit card fraud detection. J. Comput. Sci. 27, 247–254 (2018)

[95] Raza, M., Qayyum, U.: "Classical and deep learning classifiers for anomaly detection". In: Proceedings 2019 16th International Bhurban Conference on Applied Sciences and Technology, IBCAST 2019, pp. 614–618 (2019)

[96] R. J. Bolton, D. J. Hand, F. Provost, L. Breiman, R. J. Bolton, and D. J. "Hand Statistical Fraud Detection": A ReviewComment. Statistical Science, 17(3):235–255, 2002. ISSN 08834237. doi: 10.1214/ss/1042727940

[97] Pumsirirat, A., Yan, L.: Credit card fraud detection using deep learning based on auto-encoder and restricted Boltzmann machine. Int. J. Adv. Comput. Sci. Appl. 9(1), 18–25 (2018)

[98] Fiore, U., De Santis, A., Perla, F., Zanetti, P., Palmieri, F.: "Using generative adversarial networks for improving classification effectiveness in credit card fraud detection". Inf. Sci. 479, 448–455 (2017)

[99] R. Jain, B. Gour and S. Dubey,"A Hybrid Approach for Credit Card Fraud Detection using Rough Set and Decision Tree Technique", International Journal of Computer Applications, vol. 139, no. 10, pp. 1-6, 2016.

[100] Kamaruddin, S., Ravi, V.: Credit card fraud detection using big data analytics: use of PSOAANN based one-class classification. In: Proceedings of International Conference on Informatics Analytics – ICIA 2016, pp. 1–8 (2016).

[101] Askari, S.M.S., Hussain, M.A.: Credit card fraud detection using fuzzy ID3. In: Proceeding -IEEE International Conference on Computing Communication and Automation ICCCA 2017, January 2017, pp. 446–452 (2017).