Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 3 (2024)

Fraud Detection in Credit Cards Using Methods of Machine Learning

Sunita Singh Air ,Mrs. Anubhooti Papola
Veer Madho Singh Bhandari Uttarakhand Technical University, Dehradun

Abstract: The rise of technological advancements and advanced communication networks leads to increase in fraud related to credit card. The repercussions of fraud related to credit card impacting both consumers and financial institutions. Fraudsters consistently evolve their techniques, emphasizing the necessity of making fraud protection technologies essential for banks and other financial entities. This research paper presents a method for an effective credit card fraud detection by integrating a feedback system using machine learning methodology. This feedback approach aims to enhance the detection accuracy and cost-effectiveness of the classifier. The study evaluates the performance of various methods, including artificial neural networks, random forest, Naive Bayes, tree classifiers, logistic regression, support vector machines, and gradient boosting classifiers. The evaluation is conducted on slightly skewed credit card fraud datasets containing transaction data from European account holders, totaling 284,807 trades. The evaluation considers both pre-processed content and raw. The efficiency of these methodologies is evaluated based on performance assessment dimensions for different classifiers, including precision, F1-score, accuracy, recall, and the false positive rate (FPR) percentage. The findings contribute to the ongoing efforts to develop robust systems for detecting and preventing fraud related to credit card, safeguarding from substantial financial harm.

Keywords: Credit Card Fraud Detection, Methods of Machine learning, Supervised learning, Methods of Classification.

1. Introduction

In today's digital era, the availability of statistical information worldwide has become easily accessible due to online digital platforms. Information with vast volume, extensive scope, frequent occurrence, and importance is stored in the cloud by organizations of varying sizes, ranging from small to large. This information is available on various sources such as social media followers, likes, shares and customer behaviors. Crimes related to white-collar poses a growing challenge with far-reaching consequences for the corporate entities, financial sector, and governments. Fraud can be the illegal deceit to obtain financial gains[1]. Enhanced card transactions, with a strong reliance on communication technology, has amplified the complexity of the situation. Credit card transactions, both offline and online, have become the most prevalent mode of payment, making the detection and prevention of fraud related to credit card crucial. Machine learning emerges as a groundbreaking innovation that operates on massive datasets inaccessible to humans and supplants conventional strategies. Machine Learning strategies encompass into two key categories: supervised learning and unsupervised learning. Fraud detection through machine learning, depending on how it is adapted to specific datasets. Supervised learning involves recognizing anomalies based on pre-existing patterns, and numerous methods have been employed over the years to detect credit card fraud. However, a significant challenge lies in the imbalance of databases, where majority of transactions are legitimate, making it difficult to identify the extremely small number of fraudulent ones. This challenge emphasizing the need for a fraud prevention framework that is accurate, efficient, and minimizes false positives [2]. This research paper presents a method for an effective fraud detection of credit card by integrating mechanism of feedback using methods of machine learning. This feedback approach aims to enhance the accuracy and cost-effectiveness of the classifier. The study evaluates the performance of the various methods, including artificial neural networks, random forest, Naive Bayes, tree classifiers, logistic regression, gradient boosting and support vector machines classifiers. The evaluation considers both pre-processed content and raw. The research paper covering the introduction, activities related to

it, techniques for obfuscating credit card frauds, and associated challenges. Implementation of machine learning techniques addresses with the evaluation of performance measurement parameters and estimation. It concludes by presenting the research findings and proposing potential enhancements for future improvements.

2. Prior Work

Machine learning plays a vital role in various domains for efficient data management, and the detection of credit card fraud. In prior researches various methods, including supervised approach, unsupervised approach, and the hybrid approach, has been proposed to tackle this issue. The detection of credit card fraud involves interpreting card actions during purchases, and diverse strategies such as support vector machines (SVM), artificial neural networks(ANN), decision trees(DT) and genetic algorithms(GA). Credit Card Fraud detection faces challenges due to complexity of fraud behavioral models, where suspicious transactions seem to resemble genuine ones or closely resemble legitimate ones and limited accessibility to card transaction data that is both imbalanced and skewed, optimal feature selection, and the need for effective measures to evaluate the efficiency of fraud detection strategies applied Credit card fraud databases that has been distorted [5]. Effectiveness of credit card fraud detection is significantly Impacted by the choice of parameter selection, sampling approach, and identification techniques. Credit card fraud includes physically stealing a card or stealing sensitive confidential credit card details, such as card types, CVV keys and account numbers. Fraudsters use this information to attempt large transactions, making payments before the cardholder becomes aware of the manipulation of their credit card details. Due to this, businesses are employing various machine learning techniques to distinguish between legitimate and illegitimate transactions. As credit cards become common mode of transaction for both online and regular transactions, the risk of fraud also tends to rise[6]. Traditional manual methods for detecting fraudulent activities are seems to be time-consuming and prone to errors, making them less feasible for large data. The methods for detecting fraudulent activities through computing intelligence(CI) can be categorized into two categories: supervised and unsupervised methods. Supervised techniques creates models based on both fraudulent and valid transactions, to classify new entries as either fraudulent or valid. In contrast, unsupervised methods identify potential instances of fraudulent charges by detecting statistical anomalies in exchanges without relying on predefined categories [7]. In the analyzed data paper [8], experts focused on examining a hybrid data model, which includes making decisions on functionality and heuristic classification across three different levels. The initial stage includes ordinary preprocessing, while the second and third phases includes four functionality choice algorithms: data gain ratio and genetic algorithm. The hybrid model yielded outcomes with good precision. It also addressed imbalances in a credit card data collection, where legitimate transactions outnumbered fraudulent ones. This suggests that achieving an high precision rating in prediction could not effectively identify the fraudulent transactions. To address this issue, Class allocation, i.e. oversampling the minority class. By doubling class learning instances, both in oversampling the significant minority and maintaining a balanced proportion with the majority class, and the new algorithm increased the chances of accurate predictions. Supervised and unsupervised tools and techniques, highlighting the limitations of supervised optimization techniques in detecting fraud cases. Design of deep autoencoder and restricted Boltzmann machine (RBM) as methods capable of distinguishing anomalies from ordinary trends. Developing the hybrid technique such as AdaBoost and Majority Voting [9], to enhance the overall effectiveness of fraud detection. Prior studies have explored various methods to address issues related to the identification of credit card fraud. Neural network's structure is employed in an unsupervised manner for applications that facilitates processing of payment instantly. The self-arranging structure of neural network resolves the problem by categorizing each interconnected community through optical classification. This integrated approach achieves a detection rate of over 95 percent on the Receiver Operating Characteristic (ROC) curve, identifying fraudulent activities without triggering false alarms[10].

3. Methods & Challenges of Machine Learning in Credit Card Fraud Detection

Machine learning minimizes assumptions, enhances observational precision in assessing frameworks, transforming credit assessment with advanced strategies for greater accuracy.

Machine learning techniques classified as follows-

3.1 Supervised learning

It uses labeled dataset to train algorithm for a particular output. It includes initiation, detailed descriptions, support vector machines (SVM), decision trees, linear regression (LR), and neural networks that has been employed for the detection of credit card fraud [11];

- **Naive Baiyes Classifier:** It is defined as the statistical technique based on the predictive theory, which makes decisions based on the highest probability outcome. It estimates unknown outcomes from the known data using Bayesian probability, incorporating the prior knowledge and reasoning into predictions. It assumes a statistically independent relationship among features in the data.
- **Random Forest:** Random Forest (RF), developed by Leo Breiman and Adele Cutler as a trademark. Random Forest (RF) operates by aggregating predictions from the output of multiple decision trees to produce the result. It handles both classification and regression tasks.

Random forest method assist in identifying the most appropriate independent variables, enhancing model performance. Research has shown that allowing each tree to consider a subset of predictors can optimize prediction accuracy [12].

- **Logistic Regression:** It is defined as the technique borrowed from both statistical data analysis and machine learning, estimates the probability of an event occurring, where there are only two possible outcomes such as pass/fail, positive/negative. In credit card fraud detection, it utilizes probability distribution to classify transactions as fraudulent or non-fraudulent[13].
- **Support Vector Machine Classifier:** SVM, or support vector machine is a supervised machine learning model utilized for classification tasks, when dealing with binary categorizations. It employs classification learning algorithms for dividing major task into groups and individuals within labeled datasets, enabling it to effectively classify new documents based on the characteristics identified during the training process.
- **K-Nearest Neighbors (K-NN):** It is a supervised algorithm of machine learning suitable for tackling both classification and regression challenges. The prediction for a new data point is determined by majority voting among its K nearest neighbors.
- **Gradient Boosting Method (GBM):** It is also referred as the Gradient Boosting (GB) method, is a algorithm of machine learning, capable of performing both classification and regression activities. The above model consists of weak decision trees that collaborate to form a robust model that enhances predictive accuracy [15].
- **Classification Trees:** These trees records, identifies and allocates different class labels. It improves the accuracy of the classification. These trees are created using a method known as binary recursive partitioning (dividing the data recursively into two groups) [14].
- **Artificial Neural Networks (ANN) :** It is the machine learning approach inspired by the structure of the human brain and comprises of interconnected neurons. Using prior data, Artificial Neural Network (ANN) architectures can identify patterns and categorize new data.

3.2 Unsupervised learning

Unsupervised machine learning learns from data without requiring human supervision. It uses algorithms to examine and cluster unlabeled datasets. Unsupervised methods are Hidden Markov Model method (HMM), Self-organizing Map (SOM) and K- means method.

3.3 Challenges

It lies in identifying and acknowledging fraudulent transactions to ensure that merchants and customers are not billed for unauthorized transactions [17]. There are still numerous challenges that need to be tackled in Credit card fraud detection and we will discuss some of them here.

Challenges of identifying credit card fraud :

- A **vast amount** of data is accumulated daily, and the architectural framework needs to be both responsive and rapid to effectively address instances of fraud.

- The **data is skewed**, i.e. the majority of transactions (98.9%) being non-fraudulent, creates a challenge in detecting fraudulent activity.
- **Incorrectly categorized** data is an another major issue, as some fraudulent activities are unnoticed or unrecorded.

4. Implementation

Research presents an efficient detection of credit card fraud that utilizes a feedback framework based on machine learning techniques to identify fraudulent activities. The feedback mechanism improves the rate of fraud detection and efficiency of the classifier and analysis of the system's performance, comparing it with different methods such as artificial neural networks, tree classifiers, random forest, logistic regression, support vector machines, gradient boosting classifiers and Naive Bayes. The evaluation was carried out on a dataset of credit card fraud, which was notably imbalanced, consisting of 284,807 transactions from European cardholders. The machine learning methods were applied to pre-processed data and raw data, and their performance was evaluated using metrics like recall, F1-score, accuracy, precision and false positive rate(FPR) percentage.

4.1 Credit Card Database

This dataset appears to originate from the ULB Machine Learning Community, and its details can be found on the Kaggle website. The dataset comprises transactions made by credit cardholders in Europe during the year 2013, spanning two days with a total of 284,807 transactions with 492 transactions among them are recognized as fraudulent. The dataset is notably imbalanced, with features primarily associated with V1 to V28, quantity, class, time, and Principal Component Analysis (PCA). Non Principal Component Analysis based features include time, class (where 0 stands for non-fraud and 1 stands for fraud), and quantity.

4.2 Procedural Steps Involved

It outlines the process for identifying the credit card frauds as depicted in Figure 4.3. The steps involved are as follows -

1. **Data Gathering :** Collect data available and upload the credit card dataset.
2. **Data Pre-processing:** Enhance data pre-processing using one-class classifiers and the Matthews correlation coefficient to address dataset imbalances.
3. **Correlation Matrix:** Generate and analyze the correlation matrix for the dataset.
4. **Data Splitting:** Divide the dataset into training (70%) and testing (30%) subsets.
5. **Classification Methodology:** Apply classification system (Machine Learning) methodology.
6. **Evaluation Metrics Calculation:** Calculate evaluation metrics including accuracy,

f1-score, confusion matrix (Table 4.2.1), precision, recall (or True Positive Rate), False Positive Rate using their respective formulas -

Precision: Precision = $\frac{\text{True Positive}}{(\text{False Positive} + \text{True Positive})}$

Recall : Recall or True Positive Rate = $\frac{\text{True Positive}}{(\text{False Negative} + \text{True Positive})}$

F1 Score : F1 Score = $\frac{2 * (\text{Precision} * \text{Recall})}{(\text{Recall} + \text{Precision})}$

Accuracy : Accuracy = $\frac{\text{True Negative} + \text{True Positive}}{(\text{False Positive} + \text{True Positive} + \text{True Negative} + \text{False Negative})}$

False Positive Rate : False Positive Rate = $\frac{\text{False Positive}}{(\text{True Positive} + \text{False Positive})}$

Actual Value	Predicted Value	Negative (0)	Positive (1)
Negative (0)	False Negative (FN)		True Negative(TN)
Positive (1)	True Positive (TP)		False Positive(FP)

Table 4.2.1: Performance Evaluation Matrix (Confusion Matrix)

7. **Feedback Mechanisms:** Implement feedback mechanisms to enhance detections accuracy and rate.
8. **Iteration:** Iterate steps 4 to 6 for classifiers.

4.3 Approach

The working of the project is described using the following figure:

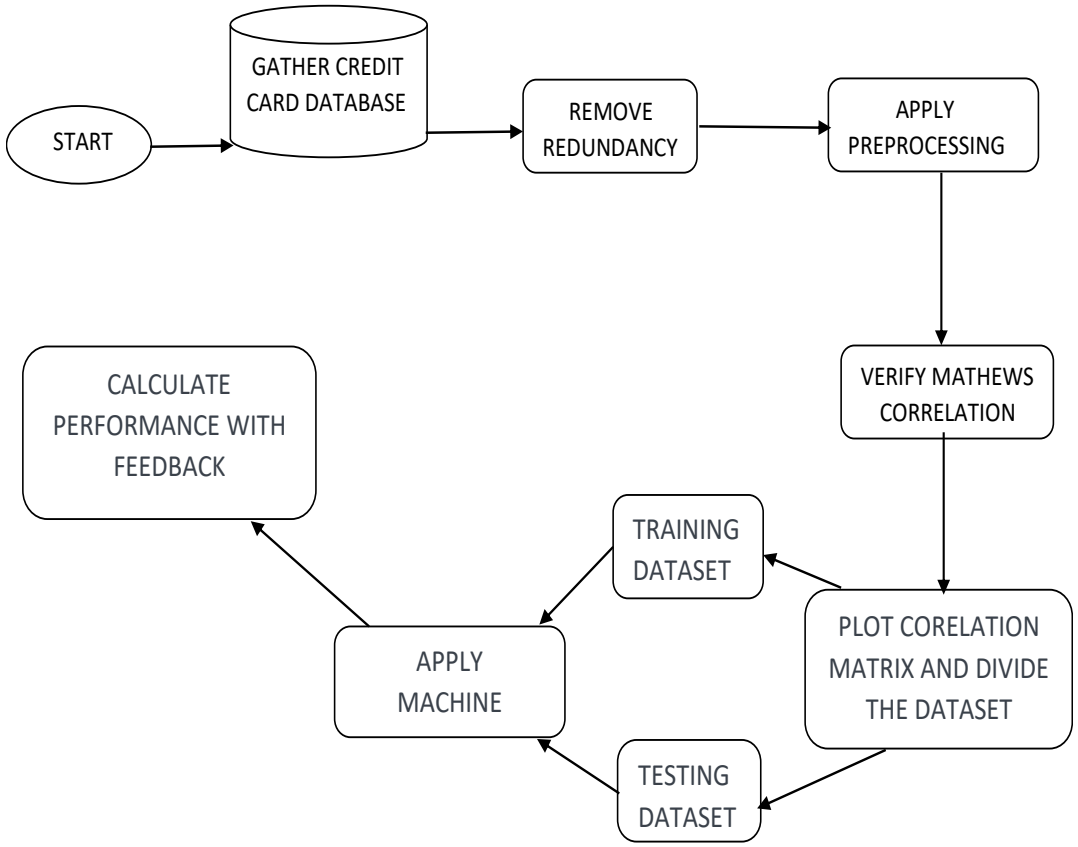

Figure 4.3 Steps in CC Fraud Detection Using Machine Learning

5. Results And Conclusion

Various performance metrics has been computed during the analysis using Python programming language to implement different algorithms of machine learning classifier for detecting frauds related to credit card in the dataset. The dataset was split into 70% for training and 30% for testing purposes.

Experimental results include calculations of various metrics for the credit card dataset. The confusion matrix displays the classification results (Class 1 for non-fraud and Class 0 for fraud). Accuracy, precision, and recall are used to assess the performance of the classifiers. Table 5.6 presents the true negative, true positive, false negative and false positive rates for each classifier in the unsampled datasets. Classifier performance varies across different evaluation metrics.

KNN Confusion matrix

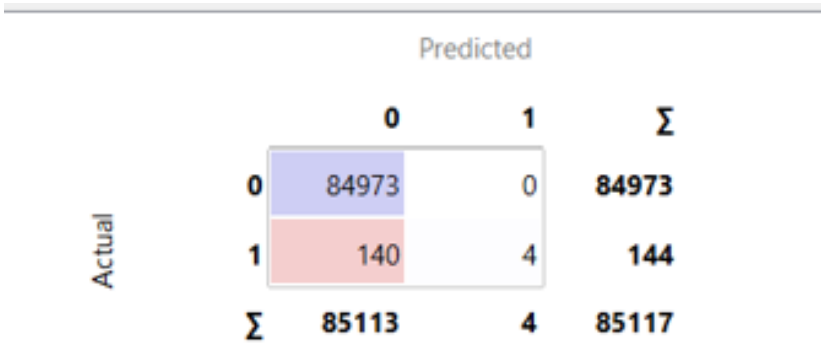

Figure 5.1

Gradient Boosting Confusion matrix

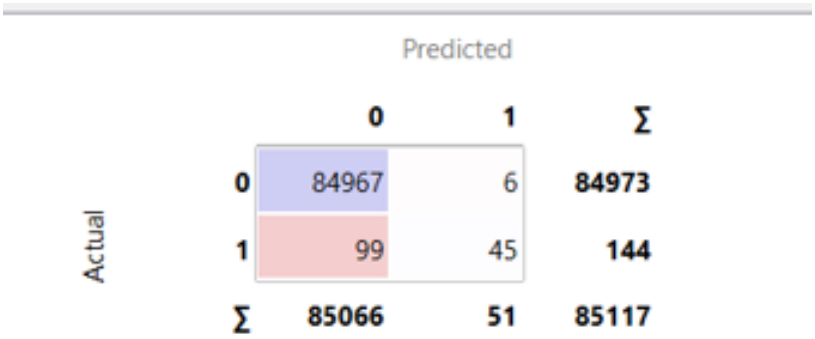

Figure 5.2

Tree Confusion matrix

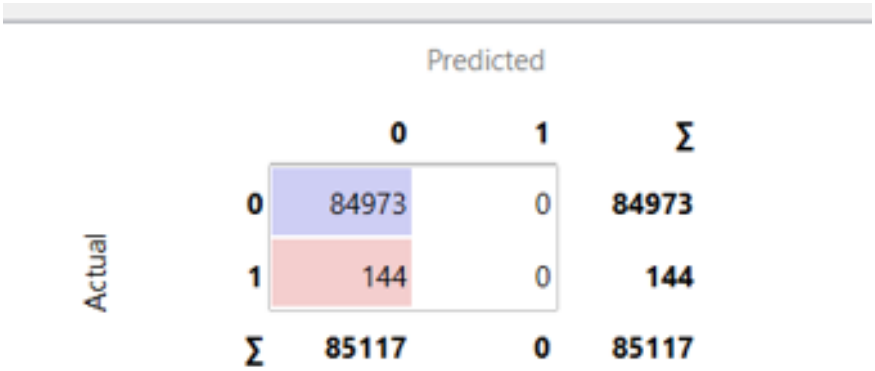

Figure 5.3

Logistic Regression Confusion matrix

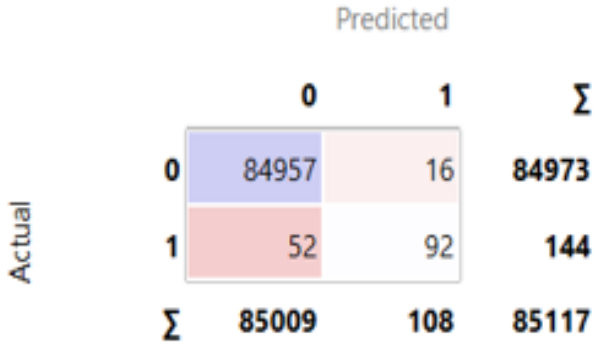

Figure 5.4

Random Forest Confusion matrix

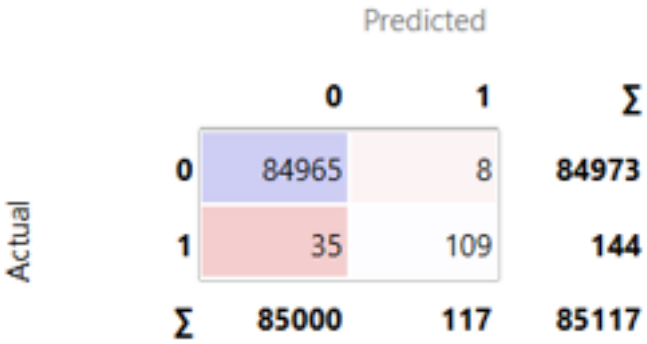

Figure 5.5

Model	Gradient Boosting	Tree	Logistic Regression	Naive Baiyes	KNN	Random Forest
Recall	0.999	0.998	0.999	0.999	0.998	0.999
Precision	0.999	0.997	0.999	0.999	0.998	0.999
F1 Score	0.999	0.998	0.999	0.999	0.998	0.999
Accuracy	0.999	0.998	0.999	0.999	0.998	0.999

Table 5.6 Results of various Methods of Machine Learning.

Results from Table 5.6 depict the evaluation metrics percentages for the dataset of credit card fraud across various methods of machine learning. The result reveal that Random Forest achieved an accuracy of 99.999 percent, Logistic Regression (LR) and Naive Bayes (NB) both achieved 99.99 percent, Decision Trees achieved 99.88 percent and Gradient Boosting Machine (GBM) achieved 99.99 percent precision in identifying credit card fraud. Higher values of precision, accuracy, F1-score and recall are generally indicative of superior performance for any machine learning technique. Among these algorithms, Random Forest (RF) stands out significantly, suggesting it can be a prudent choice for achieving higher completeness while minimizing errors.

6. Conclusion and Future Prospect

After carrying out the extensive study, the following conclusion is drawn. In addition to the conclusion, some future advancement regarding the research are also presented in detail.

6.1 Conclusion

Credit card fraud detection appears to be a complex challenge that demands a significant level of expertise, which is effectively addressed using machine learning algorithms. This serves the dual purpose of advancing both machine learning and artificial intelligence ensuring the security of customers' funds and preventing manipulation. This research includes an efficient fraud identification system based on methods of machine learning, featuring a feedback mechanism. This process of feedback enhance detection rate of the classifier's and overall effectiveness. This includes an analysis of different machine learning strategies, including artificial neural networks, random forest, support vector machines, tree classifiers, Naive Bayes logistic regression and gradient boosting classifiers. Multiple performance evaluation parameters has been calculated such as recall, F1-score, precision, false positive rate (FPR) and accuracy. Random forest outperforms other machine learning classifiers in terms of performance. Moving forward, there's potential to implement and test the proposed method on extensive real-time datasets using various additional machine learning techniques.

7. References

[1] Awoyemi, J.O., Adetunmbi, A.O. and Oluwadare, S.A., 2017, October. Credit card fraud detection using machine learning techniques: A co parative analysis. In 2017 International Conference on Computing Networking and Informatics (ICCNI) (pp. 1-9). IEEE.

[2] Adewumi, A.O. and Akinyelu, A.A., 2017. A survey of machine-learning and nature-inspired based credit card fraud detection techniques. International Journal of System Assurance Engineering and Management, 8(2), pp.937-953

[3] Fu, K., Cheng, D., Tu, Y. and Zhang, L., 2016, October. Credit card fraud detection using convolutional neural networks. In International Conference on Neural Information Processing (pp. 483-490). Springer, Cham.

[4] 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 (JTEC), 10(1-4), pp.23-27.

[5] Khan, A.U.S., Akhtar, N. and Qureshi, M.N., 2014. Real-time credit-card fraud detection using artificial neural network tuned by simulated annealing algorithm. In Proceedings of International Conference on Recent Trends in Information, Telecommunication and Computing, ITC (pp. 113-121).

[6] Carneiro, N., Figueira, G. and Costa, M., 2017. A data mining based system for credit-card fraud detection in e-tail. Decision Support Systems, 95, pp.91-101.

[7] Dhankhad, S., Mohammed, E. and Far, B., 2018, July. Supervised machine learning algorithms for credit card fraudulent transaction detection: a comparative study. In 2018 IEEE International Conference on Information Reuse and Integration (IRI) (pp. 122-125). IEEE.

[8] Adewumi, A.O. and Akinyelu, A.A., 2017. A survey of machine-learning and nature-inspired based credit card fraud detection techniques. International Journal of System Assurance Engineering and Management, 8(2), pp.937-953.

[9] Fiore, U., De Santis, A., Perla, F., Zanetti, P. and Palmieri, F., 2019. Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. Information Sciences, 479, pp.448-455.

[10] Bahnsen, A.C., Stojanovic, A., Aouada, D., and Ottersten, B., 2014, April. Improving credit card fraud detection with calibrated probabilities. In Proceedings of the 2014 SIAM international conference on data mining (pp. 677-685). Society for Industrial and Applied Mathematics.

[11] Popat, R.R. and Chaudhary, J., 2018, May. A survey on credit card fraud detection using machine learning. In 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI) (pp.

1120-1125). IEEE.

[12] Patil, S., Nemade, V. and Soni, P.K., 2018. Predictive modelling for credit card fraud detection using data analytics. Procedia computer science, 132, pp.385-395.

[13] Malini, N. and Pushpa, M., 2017, February. Analysis on credit card fraud identification techniques based on KNN and outlier detection. In 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication, and Bio-Informatics (AEEICB) (pp. 255-258). IEEE.

[14] Zareapoor, M. and Shamsolmoali, P., 2015. Application of credit card fraud detection: Based on bagging ensemble classifier. Procedia computer science, 48(2015), pp.679-685.

[15] Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C. and Bontempi, G., 2015, July. Credit card fraud detection and concept-drift adaptation with delayed supervised information. In 2015 international joint conference on Neural networks (IJCNN) (pp. 1-8). IEEE.

[16] Mahmoudi, N. and Duman, E., 2015. Detecting credit card fraud by modified Fisher discriminant analysis. Expert Systems with Applications, 42(5), pp.2510-2516.

[17] Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P.E., He-Guelton, L. and Caelen, O., 2018. Sequence classification for credit-card fraud detection. Expert Systems with Applications, 100, pp.234-245.

[18] Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C. and Bontempi, G., 2017. Credit card fraud detection: a realistic modeling and a novel learning strategy. IEEE transactions on neural networks and learning systems, 29(8), pp.3784-3797.