Scientific Research Publishing

Journal of Computer and Communications, 2024, 12, 1-11
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Credit Card Fraud Detection Using Machine Learning Techniques

Ananya Sarker, Must. Asma Yasmin, Md. Atikur Rahman, Md. Harun Or Rashid, Bristi Rani Roy

Department of Computer Science and Engineering, Bangladesh Army University of Engineering & Technology (BAUET), Natore, Bangladesh

Email: ananya.ruet@gmail.com, asma.yasmin.cu@gmail.com, atik.cse@bauet.ac.bd, harun.ruetbd@gmail.com, bristiroy.cse@gmail.com

How to cite this paper: Sarker, A., Yasmin, M.A., Rahman, Md.A., Rashid, Md.H.O. and Roy, B.R. (2024) Credit Card Fraud Detection Using Machine Learning Techniques. *Journal of Computer and Communications*, **12**, 1-11.
https://doi.org/10.4236/jcc.2024.126001

Received: May 29, 2024
Accepted: June 18, 2024
Published: June 21, 2024

Abstract

Credit card companies must be able to identify fraudulent credit card transactions so that clients are not charged for items they did not purchase. Previously, many machine learning approaches and classifiers were used to detect fraudulent transactions. However, because fraud patterns are always changing, it is becoming increasingly vital to investigate new frauds and develop the model based on the new patterns. The purpose of this research is to create a machine learning classifier that not only detects fraud but also detects legitimate transactions. As a result, the model should have excellent accuracy, precision, recall, and f1-score. As a result, we began with a large dataset in this study and used four machine learning classifiers: Support Vector Machine (SVM), Decision Tree, Naïve Bayes, and Random Forest. The random forest classifier scored 99.96% overall accuracy with the best precision, recall, f1-score, and Matthews correlation coefficient in the experiments.

Keywords

Support Vector Machine, Decision Tree, Nave Bayes, Random Forest, Matthews Correlation

1. Introduction

A credit card is a compact card that is made of thin plastic or fiber that carries information about an individual such as a photograph or a signature and allows the person identified on the card to pay the charges for purchased products or services. A credit card is linked to the bank account of an individual and therefore, expending from a credit card means automatic deduction of credits or money from the mail bank account. It can be utilized in diverse places and ser-

vices such as ATMs, swiping machines, retail readers, banks, and online transactions. Each card has a unique card number, an expiry date, and a pin code or security code. The security of the credit card depends on both the physical card and the credit card information such as the credit card number along with the pin code or security code. Credit card fraud can happen if someone steals the physical card or get access to the account virtually. As the quantity of credit card transactions grows, the number of fraudulent instances grows as well. In 2018, credit card fraud caused a total estimated loss of US $844.8 million in London. Therefore, credit card theft is on the rise and financial losses due to these frauds are increasing too.

The Internet and online transactions are becoming more popular as new technology arises. The majority of these transactions are made with credit cards. Fraud protection or detection must be introduced to reduce these losses. As technology advances at a rapid rate, new types of fraud occur. As a result, while different machine learning algorithms are used to detect frauds, hybrid algorithms and artificial neural networks are becoming more popular due to their higher performance. Researchers have worked on different data mining and statistical tools, artificial intelligence approaches, and pattern matching to detect fraudulent transactions. Recently, many works have suggested different machine learning and deep learning classifiers to detect fraudulent transactions.

The advantages of machine learning algorithms are that they are lightweight and don't need many instances of data for a correct prediction of frauds. However, the performance is not up-to-the-mark like the deep learning approaches and machine learning classifiers need hand-engineered features for a perfect identification of credit card frauds. On the other hand, deep learning approaches don't need hand-engineered features. They can figure out and extract valuable features on their own and the performance is also high. However, deep learning approaches need a lot of instances and high computation for attaining a good outcome.

Overlapping and dataset imbalance are the two major problems related with credit card transaction [1] [2]. Imbalanced data distribution is overcome using sampling methods. Sometimes the detection of credit card fraud for new frauds may be problematic if new data has drastic changes in fraud patterns [3]. It is vital to detect fraud in a method that is both effective and trustworthy. Therefore, in this study, we have applied different machine learning classifiers such as random forest, decision tree, Naïve Bayes, and support vector machine (SVM) for the prediction of fraudulent transactions. Experimental results revealed that random forest achieved an overall accuracy of 99.96% while the other approaches under consideration achieved more than 99% for the considered dataset. Therefore, we concluded that the mentioned four algorithms are suitable for detecting credit card fraud and the random forest classifier can detect the frauds almost perfectly.

The goals of credit card fraud detection are to reduce the losses of merchants and issuing banks from payment fraud while also increasing revenue potential

for merchants. The task of detecting credit card fraud is difficult for the user. Online payment does not necessitate the use of a physical card and anyone with the card's information can make the transactions. Currently, cardholders are only notified after a fraudulent transaction has been completed. There is no mechanism in place to track fraudulent transactions while the transactions are being taken place.

The overall objectives of this study are:

- To identify valid and fraud transactions.
- To compare the performance of different machine learning techniques.

2. Related Works

A lot of methods have been implemented to detect fraud using supervised, unsupervised algorithms and hybrid ones. A recent study was conducted by T. Deepika *et al*. in [4] on credit card. In their research, they proposed a method to find credit card counterfeit using k-means algorithm. Another study was conducted by W. Zhou *et al*. on Credit Card Fraud Detection Using Boundary Reconstruction in [5].

In previous research, many approaches, including supervised, unsupervised, and hybrid algorithms, were employed to detect credit card fraud. However, the forms and patterns of fraud are always evolving. It is vital to understand fraud detection technologies thoroughly. In this section, we will go through the machine learning models, algorithms, and fraud detection models used in past research.

Several algorithms like Boundary Reconstruction and Integrated Classification, Random Forest etc. are addressed for the detection of fraud in credit card [6] [7]. Fraud detection using data mining approaches that take time to process when dealing with big volumes of data. Overlap is another issue with credit card transaction data preparation. To compensate for imbalanced data distribution, sampling strategies were utilized.

Another study looked at skewed data or data that has been distorted. Fraud transactions are quite infrequent when compared to legitimate transactions (when a legitimate transaction looks to be fraudulent, or when a fraudulent transaction appears to be legitimate). It discusses the difficulties of dealing with categorical data as well as many machine learning approaches will overlook categorical data. Both the cost of fraud prevention and the cost of fraudulent activity were considered here [8].

One previous work covered class imbalance and how to cope with it, as well as working with massive datasets. The executed effort overcame these hurdles [9]. In another work, the authors employed a number of models for fraud detection. Each model employed a different algorithm. If new data showed significant changes in fraud tendencies, it will be difficult to identify credit card theft for new offences. Replacing the model is risky since machine learning algorithms take a long time to train rather than forecast [10].

In one of the previous works, the classification problem was solved using the Logistic Regression (LR) approach [11]. Gaussian Mixture Models were used to discretize fraudulent circumstances. To balance data, synthetic minority oversampling was utilized. Sensitivity analysis was used to calculate economic value.

One work suggested the Risk-Based Ensemble idea. The Naïve Bayes technique was used to eliminate implicit noise in transactions, and it may yield good results for tough data [12]. In another study, the authors highlighted a key challenge: enormous real-time data [13]. Because real-world data was secret and private, it was difficult to analyze and execute algorithms.

Fraud detection was evaluated using both benchmark and real-world data as well [14]. A summary of the approaches' advantages and disadvantages was provided. The Matthews Correlation Coefficient (MCC) was chosen as a performance metric. Noise was inserted into the data to evaluate the resilience of the algorithms. They also proved that the added noise had no effect on the majority voting method. However, all the previous works failed to obtain near accurate accuracy for the recent dataset.

3. Proposed Architecture

The work in this study began with the collection of credit card transaction data, which was then divided into the training and testing sets. The data was then preprocessed so that it could be used for feature extraction. The preprocessed dataset was then subjected to classification algorithms. Four classification approaches were used and their accuracy levels were evaluated. The steps of the working flowchart are depicted in Figure 1.

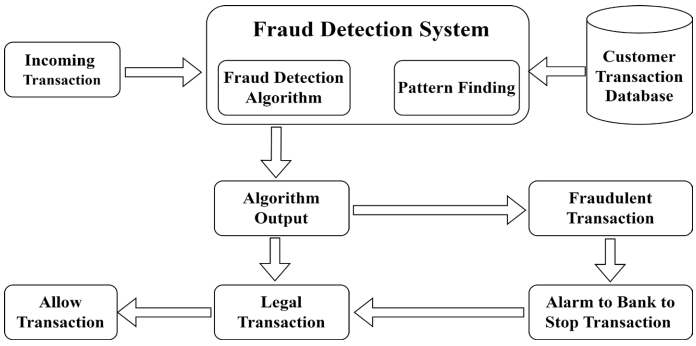

Figure 1. Workflow diagram to classify fraud transaction.

4. Methodologies

We started with collecting credit card transaction data and splitting the dataset into a training and testing set. Four classification techniques Random Forest (RF), Naïve Bayes (NB), Decision Tree (DT), and Support Vector Machine (SVM) were applied to these transaction datasets.

4.1. Dataset Description

This study made use of the Credit Card Fraud Detection dataset, which can be

obtained from Kaggle. This dataset includes transactions made by European cardholders during the period of two days in September 2013. There are 31 numerical features in the dataset. Three of the aforementioned characteristics remained constant. The dataset contained 284,807 transactions, 492 of which were fraudulent and the remaining legal.

4.2. Classification Techniques

We explain the classification techniques Random Forest (RF), Nave Bayes (NB), Decision Tree (DT), and Support Vector Machine (SVM) in this section. These categorization approaches were used to detect credit card fraud.

4.2.1. Random Forest (RF) Classifier

The Random Forest classifier [4] is composed of several tree-based structures. It can handle hundreds of input variables and performs well on huge datasets. It also calculates which variables are important for categorization. This method can assist in dealing with overfitting data items. The following is a typical approach for generating a Random Forest classifier for a dataset, D, with N occurrences and A attributes. For each iteration of construction, a candidate Decision Tree, a subset of dataset D, d, is sampled with replacement as the training dataset. An arbitrary subset of the qualities A, a, are picked as candidate attributes in a decision tree to divide the node for each node. By creating K Decision Trees in this manner, a Random Forest classifier is constructed. In this investigation, the number of estimators was set to 100, the maximum depth to 10, the random set to 0, the criteria to "Entropy", and all other parameters were kept at their default levels.

4.2.2. Decision Tree (DT) Classifier

A decision tree [9] is a basic and widely used classification approach for categorizing data. A decision tree is a tree-like structure with a root, branches, and leaf nodes. A decision tree's central node represents a test on an attribute, each branch reflects the result of a test, and each leaf node carries a class label. The root node is the top node in the decision tree. The decision tree is constructed in two stages: first, all of the training instances are assigned to the root node, and then the tree is partitioned recursively depending on specified qualities. The following step is tree trimming, which detects and eliminates branches that represent noise or outliers. Using the tree pruning method, this classification technique also solves the overfitting problem. All of the decision tree algorithm's parameters were set to default in this study.

4.2.3. Naïve Bayes (NB) Classifier

The algorithm of Naïve Bayes is a probabilistic classifier. The Bayes theorem underpins this classifier. Because of its simplicity, this classifier is particularly useful for huge datasets and is extensively used. A Naïve Bayes classifier is made up of two parts: quantitative and qualitative. The quantitative components of the Naïve Bayes classifier may be represented as network parameters termed condi-

tional tables, and the qualitative components can be represented as network structure. The probability equation is as follows:

$$P\left(\frac{A}{B}\right)=\frac{P\left(\frac{B}{A}\right)P(A)}{P(B)} \tag{1}$$

P(A/B) is the conditional probability of occurrence of event A given event B, P(B/A) is the likelihood, which is the probability of predictor given class, P(A) is the class prior probability, and P(B) is the predictor prior probability. All of the Naïve Bayes Classifier'settings were set to default in this study.

4.2.4. Support Vector Machine (SVM) Classifier

The Support Vector Machine (SVM) [5] is a linear model for classification and regression issues. This classifier is capable of solving a wide range of linear and non-linear practical situations. It generates a hyperplane that divides the data set into classes. SVM may also be applied to multi-class classification issues. The hyperplane employed in the categorization of two classes is depicted in Figure 2. While implementing the Support Vector Machine method in this study, the multiclass was set to "crammer singer", the random state was set to none, and all other parameters were left at their default values, and this algorithm provides more accuracy.

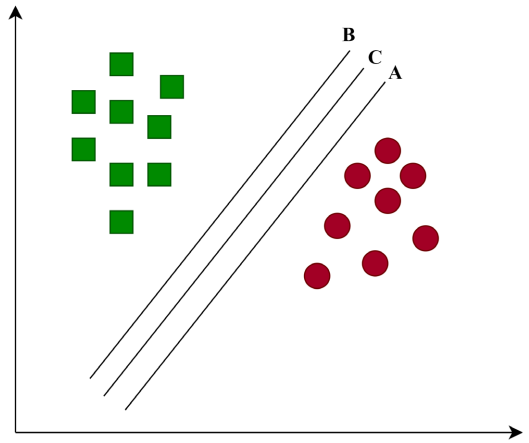

Figure 2. Hyper-plane used for classification in SVM.

5. Result Analysis and Discussion

The considered dataset included 284,807 transactions, 492 of which were fraudulent and the rest were legitimate. We can observe from the numbers that this dataset is severely skewed, with only 0.173 percent of transactions being classified as fraudulent. Among the 31 features, Class has only two values: 1 in the case of a fraud transaction and 0 otherwise. A portion of PCA dataset is shown in Figure 3. The most basic performance statistic is accuracy, which is just the percentage of properly predicted observations to all observed data. One can assume that our model is the best if it has a high level of accuracy. Although accuracy is a valuable statistic, it is only applicable when the datasets are symmetric

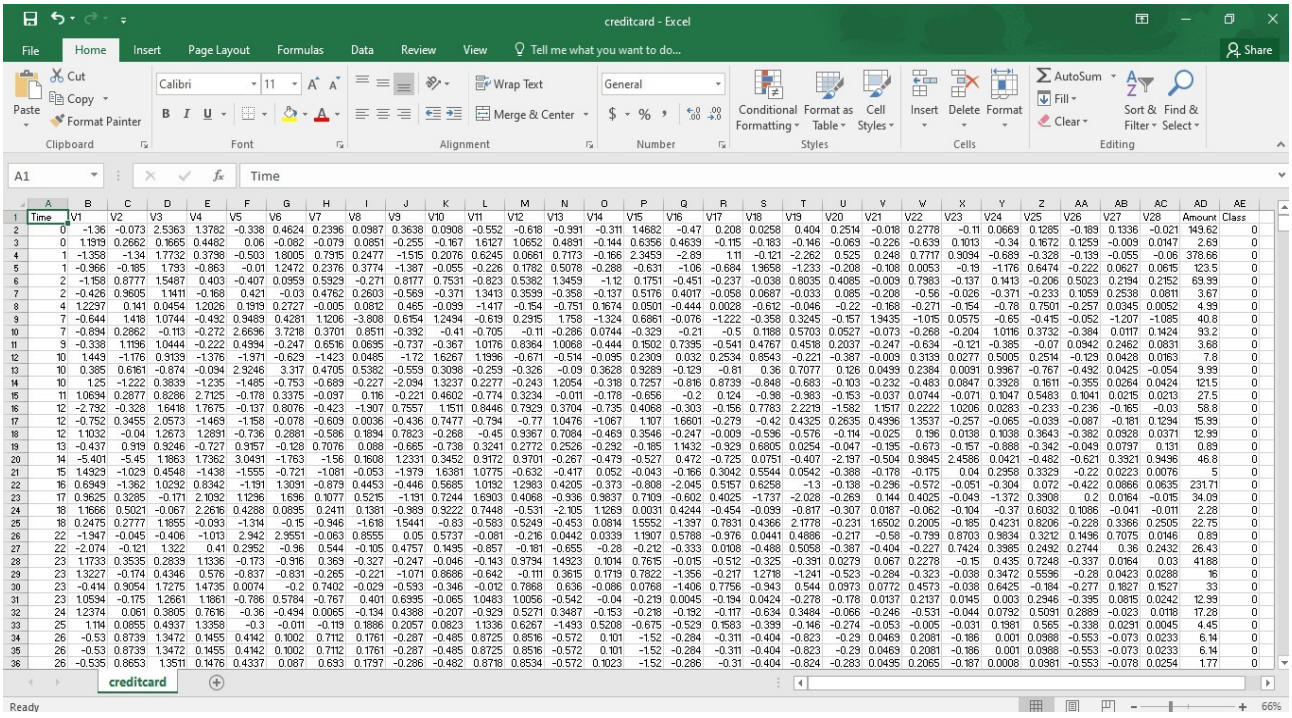

Figure 3. Credit card PCA dataset.

and the false positive and false negative values are almost equal. As a result, other parameters must be considered while evaluating the models' performance. The following figures (Figures 4-7) represent the confusion matrix for each of the applied techniques.

The proposed technique achieved 99.96 percent accuracy, implying that the proposed model is about 99.96 percent correct. The following table (Table 1) illustrates the obtained performance by all four considered classifiers.

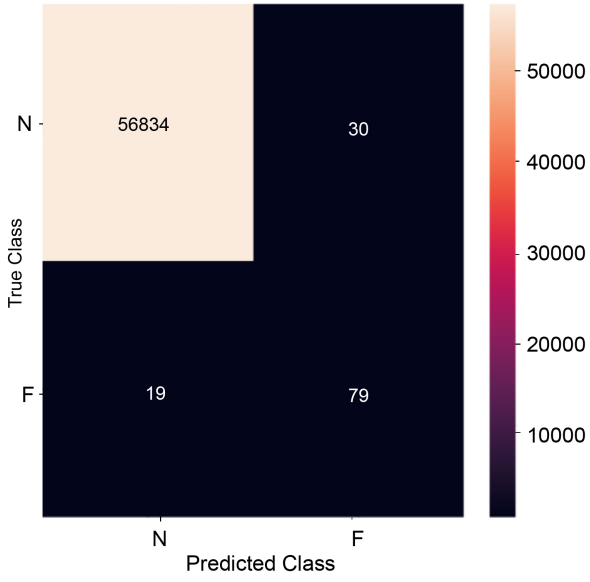

Figure 4. Confusion matrix for random forest.

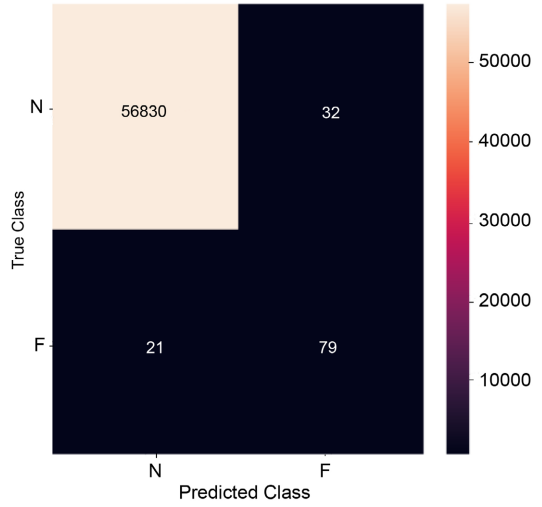

Figure 5. Confusion matrix for decision tree.

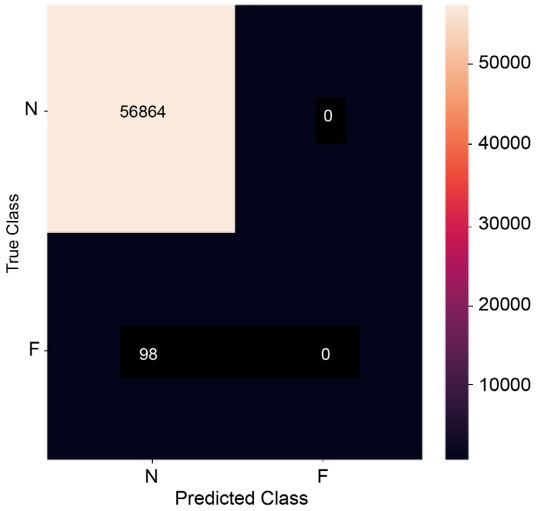

Figure 6. Confusion matrix for SVM.

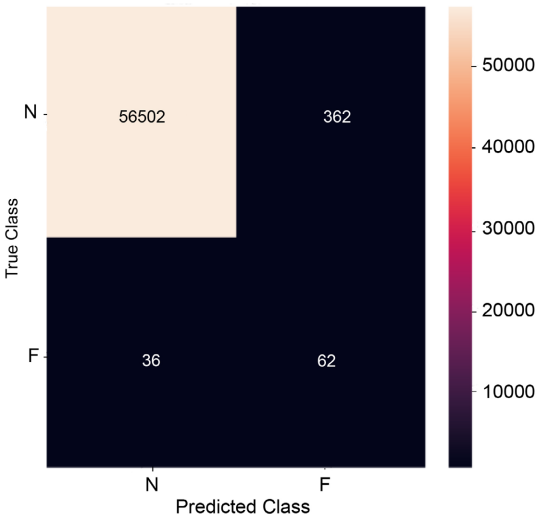

Figure 7. Confusion matrix for Naïve Bayes.

Table 1. Accuracy, Precision, Recall, F1-Score and Matthews Correlation comparison table for different ML algorithms.

Algorithms	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Matthews Correlation
Random Forest	**99.96**	**97.43**	77.56	**86.36**	**86.36**
Decision Tree	99.91	72.47	**80.61**	76.32	76.39
SVM	99.30	14.62	63.26	23.75	30.19
Naïve Bayes	99.30	14.62	63.26	23.75	30.19

The following variables are compared: accuracy, precision, recall, f1-Score, and Matthews correlation. According to the **Table 1**, the Random Forest (RF) Classifier model has the highest accuracy, precision, recall, f1-Score, and Matthews correlation. Accuracy is achieved using many methods, with the Random Forest (RF) Classifier model providing the best accuracy. The confusion matrix revealed that all approaches have a low false-positive rate, which is necessary to accomplish the aim.

The below figure (**Figure 8**) make a comparison on existing testing set and proposed testing set with some of the related works [15]-[17].

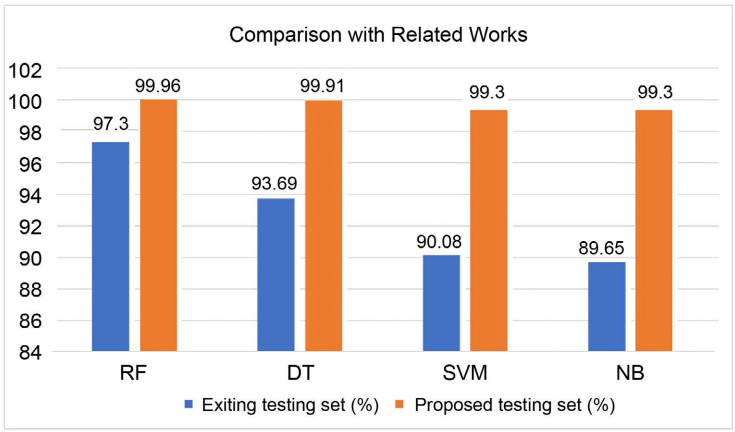

Figure 8. Comparative analysis of the related works.

6. Conclusion

Credit card fraud is a common problem that causes both individuals and banks and credit card firms to lose money. This project intends to aid consumers and banks in recovering their income by constructing a model that can more efficiently identify fraudulent and non-fraudulent transactions using the time and amount variables in the Kaggle dataset. We start by building the model with supervised machine learning methods like the random forest, decision tree, support vector machine, and Naïve Bayes. In this study, we presented a procedure to address this issue statement. We used all four machine learning classifiers, and the results showed that the Random Forest classifier had the greatest accuracy, precision, recall, and f1-score. As a result, it is the greatest choice for detecting

fraudulent transactions. In the future, we will concentrate on other datasets and machine learning approaches to get a more efficient solution.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Xuan, S., Liu, G., Li, Z., Zheng, L., Wang, S. and Jiang, C. (2018) Random Forest for Credit Card Fraud Detection. 2018 *IEEE* 15*th International Conference on Networking, Sensing and Control* (*ICNSC*), Zhuhai, 27-29 March 2018, 1-6. https://doi.org/10.1109/icnsc.2018.8361343

[2] Vats, S., Dubey, S.K. and Pandey, N.K. (2013) A Tool for Effective Detection of Fraud in Credit Card System. *International Journal of Communication Networks and Security*, **2**, 25-29. https://doi.org/10.47893/ijcns.2013.1062

[3] Patel, R.D. and Singh, D.K. (2013) Credit Card Fraud Detection & Prevention of Fraud Using Genetic Algorithm. *International Journal of Soft Computing and Engineering*, **2**, 292-294.

[4] Deepika, T. and Manimekalai, S. (2022) A Novel Method to Find Credit Card Counterfeit Detection Using K-Means Algorithm. *Journal of Algebraic Statistics*, **13**, 1125-1130.

[5] Zhou, W., Xue, X. and Luo, D. (2022). Credit Card Fraud Detection Using Boundary Reconstruction and Integrated Classification. 2022 4*th International Conference on Big Data Engineering*, Beijing, 26-28 May 2022, 86-93. https://doi.org/10.1145/3538950.3538962

[6] Rigatti, S.J. (2017) Random Forest. *Journal of Insurance Medicine*, **47**, 31-39. https://doi.org/10.17849/insm-47-01-31-39.1

[7] Suthaharan, S. (2016) Science of Information. In: Suthaharan, S., Ed., *Machine Learning Models and Algorithms for Big Data Classification*, Springer, 1-12.

[8] Soltani, N., Akbari, M.K. and Sargolzaei Javan, M. (2012). A New User-Based Model for Credit Card Fraud Detection Based on Artificial Immune System. *The* 16*th CSI International Symposium on Artificial Intelligence and Signal Processing* (*AISP* 2012), Shiraz, 2-3 May 2012, 29-33. https://doi.org/10.1109/aisp.2012.6313712

[9] Webb, G.I., Keogh, E. and Miikkulainen, R. (2010) Naïve Bayes. In: Sammut, C. and Webb, G.I., Eds., *Encyclopedia of Machine Learning*, Springer, 713-714.

[10] Ozçelik, M.H., Duman, E., Isik, M. and Cevik, T. (2010). Improving a Credit Card Fraud Detection System Using Genetic Algorithm. 2010 *International Conference on Networking and Information Technology*, Manila, 11-12 June 2010, 436-440. https://doi.org/10.1109/icnit.2010.5508478

[11] Yu, W. and Wang, N. (2009). Research on Credit Card Fraud Detection Model Based on Distance Sum. 2009 *International Joint Conference on Artificial Intelligence*, Hainan, 25-26 April 2009, 353-356. https://doi.org/10.1109/jcai.2009.146

[12] Myles, A.J., Feudale, R.N., Liu, Y., Woody, N.A. and Brown, S.D. (2004) An Introduction to Decision Tree Modeling. *Journal of Chemometrics*, **18**, 275-285. https://doi.org/10.1002/cem.873

[13] Stolfo, S.J., Fan, W., Lee, W., Prodromidis, A., and Chan, P.K. (2000) Cost-Based Modeling for Fraud and Intrusion Detection: Results from the JAM Project. *Pro-*

ceedings DARPA Information Survivability Conference and Exposition. DISCEX'00, Hilton Head, 25-27 January 2000, 130-144.

[14] Prodromidis, A.L. and Stolfo, S. (1999) Agent-Based Distributed Learning Applied to Fraud Detection. Department of Computer Science, Columbia University.

[15] Borah, L., Saleena, B. and Prakash, B. (2020) Credit card Fraud Detection Using Data Mining Techniques. *Seybold Report*, **15**, 2431-2436.

[16] Meenakshi, B.D., Janani, B., Gayathri, S. and Indira, N. (2019) Credit Card Fraud Detection Using Random Forest. *International Research Journal of Engineering and Technology* (*IRJET*), **6**, 2019.

[17] Sahin, Y. and Duman, E. (2011). Detecting Credit Card Fraud by ANN and Logistic Regression. 2011 *International Symposium on Innovations in Intelligent Systems and Applications*, Istanbul, 15-18 June 2011, 315-319. https://doi.org/10.1109/inista.2011.5946108