Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 190 (2021) 178–183

Procedia Computer Science

www.elsevier.com/locate/procedia

2020 Annual International Conference on Brain-Inspired Cognitive Architectures for Artificial Intelligence: Eleventh Annual Meeting of the BICA Society

Identification of non-typical international transactions on bank cards of individuals using machine learning methods

Jenny Domashova[a*], Elena Kripak[b]

[a]National Research Nuclear University "MEPhI", 31 Kashirskoe shosse, Moscow 115409, Russia
[b]Federal State Budgetary Educational Institution of Higher Education "Orenburg State University", 13 pr.Pobedy, Orenburg, 460018, Russia

Abstract

The growing popularity of payment cards has led to the emergence of new types of illegal transactions with money. In particular, the widespread use of non-cash payments has allowed fraud to reach the international level. Therefore, financial institutions are interested in the development and implementation of new effective fraud monitoring systems that will minimize the risk of approving illegal transactions. The article presents the results of applying machine learning methods to detect fraudulent transactions with bank cards. The use of various classification methods in modeling the specified problem is investigated. Generalized algorithm for detecting fraudulent transactions has been developed, which makes it possible to detect atypical international money transfers in real time. Generalized algorithm for detecting atypical international transfers will allow timely detection of potential fraud cases, thereby reducing the total volume of losses from illegal transactions and minimizing the reputation damage caused to the organization.

Keywords: suspicious transactions; non-typical transactions; anti-fraud system; machine learning; classification methods.

* Corresponding author: Jenny Domashova.
E-mail address: janedom@mail.ru

10.1016/j.procs.2021.06.023

1. Introduction

The financial technology market is one of the fastest growing in the world. More and more people prefer non-cash payments using bank cards. However, the increase in popularity of payment cards has led to the emergence of new types of illegal cash transactions. In particular, the ubiquity of non-cash payments has allowed fraud to reach the international level, and losses from illegal transactions are increasing from year to year. [1]

In this regard, banking organizations, money transfer and payment operators are obliged to identify such cases of illegal transactions. In addition, the high level of customer fraud negatively affects the company's business reputation, and hence, organizations are interested in developing and implementing effective fraud monitoring systems, which will minimize the risk of approval of illegal transactions. [2]

In order to help financial organizations safely process card payments and reduce the likelihood of card fraud, a special Payment Card Industry Data Security Standard (PCI DSS) has been created. The standard strengthens control of information about cardholders. [3]

Therefore, the problem of developing a generalized algorithm for the detection of atypical international transactions on bank cards of individuals to optimize methods for the detection of fraud transfers is considered relevant. [4]

2. Materials and Methods

To solve the problem, a number of procedural steps are necessary: perform a comparative analysis of existing algorithms to detect potential fraud; consider different data classification algorithms in terms of evaluating the results of their work on unbalanced dataset; form a feature space; develop an algorithm for detecting atypical transfers; implement the developed algorithm and evaluate the quality of its work.

Currently, to detect illegal transactions, existing anti-fraud systems use payment information (such as amount and direction of transfer), data on bank cards, involved in the transaction, information about the device from which the payment was made, information about the location of the sender at the time of the transfer, etc. In addition, fraud monitoring systems often accumulate information about the history of payments of a particular user on a certain card cash withdraw and deposit accounts. This allows to detect cases of atypical operations in different directions of transaction. [5]

Fraud prevention systems are the first level of protection of information technology systems against illegal transactions with money and other property. The primary objective of this stage is to prevent fraudulent transactions. Mechanisms at this level are aimed at preventing cyber attacks at both the hardware and software levels. In addition to preventing unauthorized access, they also allow organizations to implement network security policy for traffic between the internal network and the Internet. Algorithms of encrypting personal data about users and their transactions can be used to protect information within the organization. However, fraud prevention systems are not always effective and are exposed to numerous threats.

The next level of protection against fraud attempts is the fraud detection system. This type of systems serves to detect and identify illegal actions aimed at breaking into the organization's security systems and to report such actions to the system administrator in real time. Such systems are based on pre-defined rules for suspicious transactions detection established by experts, which significantly reduces the effectiveness and practical significance of this type of systems. Therefore, to detect fraud transactions more effectively, algorithms that allow both known fraud schemes and new ones to be detected are required.

In solving fraud detection tasks, two basic approaches are generally applied. In the static method of training, the detection model is periodically retrained from scratch (e.g. once a year or month). In the real-time method of learning, the detection model is updated every time new data is received.

Intelligent data analysis has several significant advantages over other methods of combating fraud:

- hypothetical fraud schemes are built on the basis of analysis of all available data about users and their transactions
- probability that each particular transaction will subsequently prove fraudulent is calculated , therefore, it is possible to prioritize cases for fraud investigation

- new fraudulent algorithms unknown before are discovered

Therefore, machine learning methods are currently widely studied to combat fraud.

Credit card transaction databases usually include a combination of numerical and categorical features. New features can also be created by aggregating information on cardholders' transactions for certain periods of time.

Recently, the most popular solutions to fraud detection tasks combine approaches to anomaly detection and classification methods. Other ways to detect illegal transactions may be clustering algorithms.

In general, the process of detecting atypical transactions consists of three stages:

- data preprocessing, which includes data clearance and the formation of a feature space
- direct training of selected machine learning models
- evaluation of the results of the obtained models and selection of the best one

A general algorithm for detecting atypical transactions is presented in Figure 1.

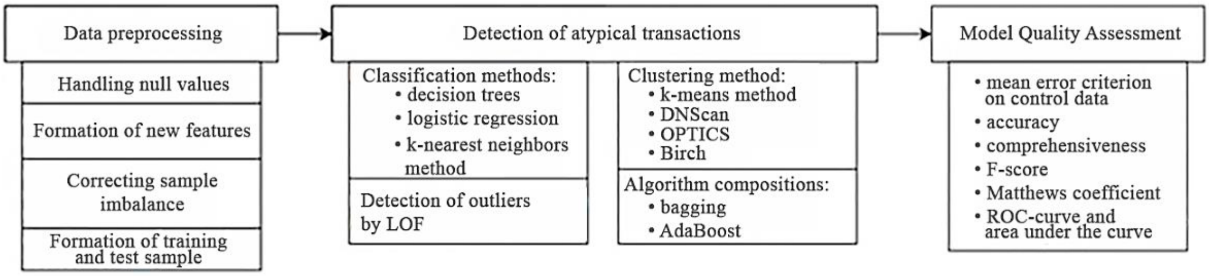


Figure 1 - General algorithm of detection of fraudulent transactions

It is necessary to consider the problems that are observed in the domain. One of them is the problem of unbalanced sampling in a changing environment, and the other is the lack of available transaction data due to confidentiality restrictions, which do not allow the dissemination of real data sets to evaluate existing methods and to analyze ways of further development in this area.

Modeling on unbalanced datasets remains a challenging task, since most existing machine learning algorithms are still not suited to solve problems with uneven distribution of objects between classes. Traditional classification methods with unbalanced datasets are most often based on different sampling methods used to balance the base sample.

Two main approaches are identified among the ways to solve this problem. Sample balancing methods working at the data level are used at the preprocessing stage of the source datasets to correct the bias in the number of objects belonging to different classes towards the minority class, as well as to remove noise objects that are located on the boundaries between different classes. In addition, there are also a number of classification algorithms designed to work on unbalanced samples.

Typically, sample balancing methods do not take into account any specific information about objects in the source set when removing or adding observations from a single class, but they are easy to implement.

Tomek links search algorithm removes the overlap between classes by removing major class objects until any pair of the nearest neighbors will not be from the same class. [6]

The synthetic minority oversampling technique (SMOTE) is one of the balancing algorithms, which increases the number of minority class objects by random data replication, until the number of objects in classes becomes comparable. The SMOTE algorithm determines the k nearest neighbors for each object of the minority class, then artificially adds redundant observations representing convex linear combinations of all k nearest neighbors of the object of the minority class. [6]

Artificial observations create larger and less specific areas of data used for decision-making. Thus, minority-class objects are studied separately, which reduces their likelihood of being classified in the majority class.

Classification is the task of distributing the set of objects to homogeneous pre-known groups, it is considered an example of teaching with a teacher, i.e. training, where a learning set of correctly identified observations is available. The relevant uncontrolled procedure, known as clustering, includes grouping data by categories on the basis of some measure of inherent similarity or distance.

In machine learning, ensemble classification methods use several algorithms at once instead of using an individual learning algorithm to obtain a greater predictive ability.

The basic algorithms that make up the composition must different substantially, so that the drawbacks of individual algorithms can be compensated. Outliers are the basic form of non-standard behavior that can be used to detect fraud. The observation, which differs significantly from other observations, is suspicious.

3. Result

The source data set was formed using SQL queries to the transaction database. The selection consists of 1,328,974 observations, 1,638 of which are fraud and 1,328,974 are legitimate transactions. Data contains transaction information (*country of payment, amount of transfer in USD*, *date and time of transfer*, *country of the withdrawal card issuer*, *bank identification number (BIN) of the withdrawal card*, *sender currency*, *country of the deposited card issuer*, *recipient currency*, etc.) and user information (*date of registration in the service*, *account country*, *country of registration*, *date of birth*, *total number of payments*, *number of successful payments*, etc.)

New features were formed during data preprocessing.

Since the time stamp itself does not carry any meaningful information, the following were calculated:

- age of the client at the time of registration
- age of the client at the time of the transfer
- the time elapsed from the moment of registration to the execution of the transfer

Since the dataset contains 249 different countries (regions from which or to which transfers are possible), it seems logical to divide these values into several groups.

4. Discussion

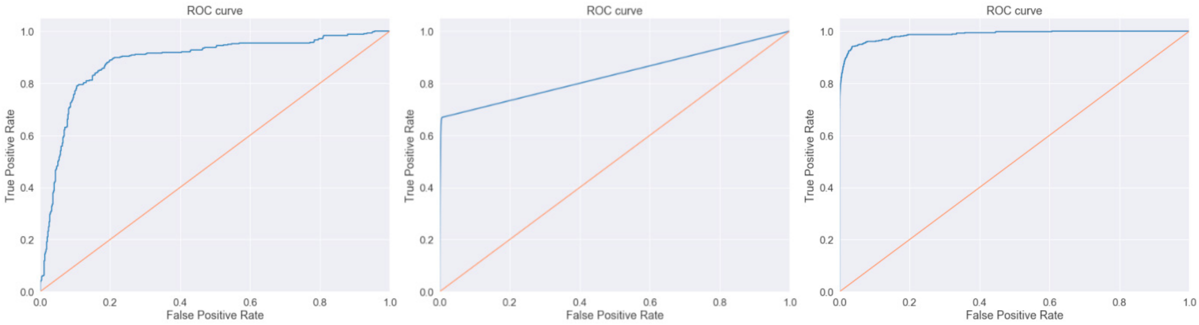
Unsupervised learning algorithms have not produced any satisfactory results. It can be assumed that this is due to the fact that fraudsters try to hide illegal transfers among a large number of legitimate transactions, so fraud transfers do not differ significantly from legal ones.

The assessment of the quality of classification by various methods to detect fraudulent transactions is presented in table 1.

Table 1. Evaluation of the quality of classification by different methods.

Method	Accuracy	Precision	Recall	F-score	MCC	AUC
Logistic regression	0.814	0.899	0.652	0.756	0.633	0.852
Bagging	0.998	0.144	0.379	0.209	0.233	0.832
AdaBoost	0.999	0.629	0.821	0.712	0.718	0.987
Local Outlier Factor	0.988	0.017	0.002	0.004	0.002	0.503

ROC curves on the test sample for algorithms: a) Logistic regression; b) Bagging; c) AdaBoost are shown in Figure 2.



a) b) c)

Figure 2 - ROC curves on the test sample for algorithms: a) Logistic regression; b) Bagging; c) AdaBoost

Among the classification algorithms, the best result was the ensemble method AdaBoost with decision trees as basic classifiers. The algorithm gave false positive results in 197 cases, false-negative results in 73, and correctly classified 335 cases of fraud, contained in the test sample. It is worth to note that the method of outliers' detection tends to provide false positive answers (13,861 legitimate transactions have been marked as fraudulent). This may be related to the fact that some users can make a one-time large transfer, which are out of the total mass of transactions.

The most important features for the classification were *the time elapsed from registration to payment*, *the distance from registration point to the payment point*, *the country of the issuer and the bin of the withdrawal card*, as well as *the number of successful payments made by the user*. At the same time, the dependency between these features is also important. Thus, fraudulent transfers are characterized by a short time elapsed since registration (transfers are made within one to two minutes after registration, and in general accounts are used no longer than a month) and the distance from the registration point to the payment point can exceed 2.5 thousand kilometers (for legitimate transfers the average distance is about 477 km).

On average, 57 successful transfers of 80 (72%) are made from law-abiding users accounts and 7 out of 16 (45%) from fraud accounts. Unsuccessful payments are considered to be those canceled by the users themselves, those in which the sender's bank rejected the debiting or the recipient's bank rejected the crediting, or transfers are stopped by the company's anti-fraud system

Among the countries with the largest number of fraud transactions are the United States, the United Kingdom, Israel, Germany, Belgium, Canada and the Russian Federation. At the same time, it is also necessary to take into account the direction of the payment. Most of the illegal transfers were sent to African countries, Russia and Ukraine.

5. Conclusion

Anti-fraud systems that currently exist do not have sufficient flexibility to adapt to organizations business processes of. In addition, the unbalanced sample complicates the classification task, and the clustering algorithms for detecting outliers have not yielded positive results. Therefore, random sampling, SMOTE and Tomek links methods were used in order to balance the sample. The optimal classification algorithm was the AdaBoost composition with decision trees as the base classifiers.

The application of the developed algorithm made it possible to correctly classify 451 suspicious transactions from the test sample, giving a false-positive result in 38 cases, so it can be used for implementation in the operational activities of interested organizations.

The practical significance of the work is that the algorithm developed to detect atypical international transfers will allow to detect cases of potential fraud in a timely manner, thus reducing the total amount of damages from illegal transactions and minimizing the reputation damage caused to the organization.

Thus, the study proposed a generalized classification algorithm that allows to detect atypical international transfers in real time. It is based on a composition of AdaBoost algorithms with decision trees as basic classifiers. This algorithm can be used in banking sector organizations as well as in a number of other financial organizations.

Acknowledgements

This work is supported by the National Research Nuclear University "MEPhI".

References

[1] Klimov V.V., Kuzin M.V., Shchukin B.A. Monitoring of fraudulent transactions using neural network committees [Electronic resource] // Security of information technologies: electron. scientific. zhurn. 2015. №1. URL: https://bit.mephi.ru/index.php/bit/article/view/127.

[2] Abdallah A., Maarof M.A., Zainal A. Fraud Detection System: A survey. [Electronic source] // Journal of Network and Computer Applications. 2016. №68. URL: https://www.researchgate.net/publication/301307481_Fraud_Detection_System_A_survey.

[3] PCI Security Standards Council. Official site [Electronic source] // URL: https://www.pcisecuritystandards.org.

[4] Federal Trade Commission. Consumer Sentinel Network Data Book 2019 [Electronic source] // URL: https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2019.

[5] Chaudhary K., Mallick B., Yadav J. A review of Fraud Detection Techniques: Credit Card [Electronic source] // International Journal of Computer Applications. 2012. Vol.45 URL: https://www.ijcaonline.org/archives/volume45 (accessed on 12.10.2020).

[6] Seeja K.R., Zareapoor M. FraudMiner: A Novel Credit Card Fraud Detection Model Based on Frequent Itemset Mining [Electronic source] // The Scientific World Journal. 2014. URL: https://www.researchgate.net/publication/266746615_FraudMiner_A_Novel_Credit_Card_Fraud_Detection_Model_Based_on_Frequent_Itemset_Mining.

Authors

1. Jenny Domashova, Ph.D. (Econ.), Associate Professor, Institute of Financial Technology and Economic Security, NRNU "MEPhI", Moscow, Russia, janedom@mail.ru, ORCiD 0000-0003-1987-8553
2. Elena Kripak, Ph.D. (Econ.), Associate Professor, Department of Mathematical Methods and Models in Economics, Federal State Budgetary Educational Institution of Higher Education "Orenburg State University", Orenburg, Russia, kripak_e@mail.ru, ORCiD 0000-0002-7578-1353.