Сучасний стан наукових досліджень та технологій в промисловості. 2024. №4 (30)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

UDC 004.056.5
DOI: https://doi.org/10.30837/2522-9818.2024.4.031

S. GAVRYLENKO, O. ABDULLIN

IMPROVING THE ACCURACY OF MACHINE LEARNING MODEL FOR FRAUD TRANSACTIONS WITH COMBINED METHODS FOR TRANSACTION ANALYSIS

Subject matter*:* The study focuses on the methods for detection fraud transactions. **Goal***:* Improve the accuracy of machine learning models for fraud transactions with combined methods for transaction analysis. **Tasks**: Investigate methods of detection fraud transactions and suggest methods that improve accuracy. **Methods**: artificial intelligence methods, machine learning. **Results***:* Methods for detecting fraudulent transactions are investigated. Methods based on data classification technology are considered: XGBoost, SVC, Logistic Regression, Logistic Regression, AdaBoostClassifier, K-Nearest Neighbors, Isolation Forest and their software models are built. The dataset used is "creditcard.csv", which contains transactions made by European cardholders over two days and contains 492 fraud cases out of 284,807 transactions. The best result is obtained with the model based on gradient boosting, which allows to process unbalanced data. It is obtained that the f1-score, due to the use of the weight parameter of the minority class, is 86% for the minority class. To improve the accuracy of fraud detection, the labeled data was clustered into subclasses using the k -means method. The number of clusters equal to twelve was determined by the elbow method. This made it possible to improve the accuracy of multiclassification. F1-score ranges from 96 to 100% for different subclasses. The feature importance within each subclass is evaluated by the gradient boosting algorithm. The results of the experiment showed a different influence of features on subclass belonging, which allows for a more detailed analysis of the data to identify hidden structures in the data. **Conclusions***:* The scientific novelty of the results obtained is the combined use of data classification and clustering methods to detect fraudulent transactions, which reduced the number of type II errors. Assessing the informative value of features within different types (subclasses) of fraudulent transactions allows us to evaluate which features have the greatest impact on the object's belonging to a particular subclass.

Keywords: machine learning; fraud transactions; classification; clustering; feature importance.

Introduction

Payment fraud is currently one of the most popular criminal activities aimed at unlawfully obtaining confidential information for the purpose of stealing and misappropriating other people's money. There are a variety of fraud scenarios, including: cash assistance fraud scenarios, online trading, telephone fraud, hacking of social media and messenger accounts, and the creation of fake mobile applications.

Fraud has increased during russia's military aggression [1]. For example, under the guise of the social platform eDopomoha, the public service portal Diia, international organisations, and well-known Ukrainian brands, fraudsters offer citizens affected by the war to receive a cash payment on social media and messengers [2]. Later on, they lure out payment card details or online banking accounts and steal the funds. In addition, the scammers create fake mobile applications and place them on Google Play and the App Store, where the victim enters their payment card details. Fraudsters also hack into users' Instagram, Facebook, Telegram, Viber accounts and send disinformation, malware, messages asking for money, spreading, etc. [3]. Increased fraud is also dangerous in the real estate sector [4].

Detecting payment fraud is a critical task for financial institutions and e-commerce and requires continuous improvement of security systems.

To train a model effectively, large amounts of high-quality data are required. This is very difficult to obtain due to privacy regulations, fragmented data sources, or incomplete records. In addition, striking a balance between accuracy and minimising false positives is a significant challenge. False positives mark legitimate transactions as fraud, leading to customer dissatisfaction. In addition, many machine learning models, especially deep learning algorithms, function as black boxes. In this case, it is difficult to understand how they make decisions, which can be problematic, especially in the financial sector. In addition, fraudsters are constantly developing new and more sophisticated tactics, which makes them difficult to identify [5]. This requires constant updating of models, as the current level of development of fraud detection tools cannot guarantee effective information protection.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2024. No. 4 (30)

Problem statement and review of scientific publications

A wide range of machine learning methods are used to detect payment fraud, based on classification, clustering, association analysis, and data anomaly detection models [6].

Classification models use supervised learning based on labelled data to train and subsequently separate transactions into fraud and legitimate ones [7]. Neural network models also help to identify nonlinear relationships between variables [8]. Decision tree models make decisions based on a sequence of checks. Ensemble classifiers improve classification accuracy [9]. The key disadvantage of such models is that if a specific case of fraud is not presented in the training data, the model may not detect it. In addition, due to insufficient detail of transaction data, real and fraud transactions overlap, which leads to a decrease in the quality of the model. Another disadvantage of such models may be their retraining, which requires regularisation of their parameters.

Models based on unsupervised learning continuously process and analyse unlabeled data to detect patterns and build models that can identify unusual behaviour [10]. However, due to the lack of detail in transaction data, real and fraud transactions overlap, which leads to a decrease in model quality.

Expert systems create a profile of normal user behaviour for further comparison with new transactions. They are aimed at tracking changes in user behaviour that may indicate fraud activities [11]. The disadvantage of such systems is the problem of determining thresholds that balance the probability of the first and second type of error.

Associative analysis algorithms are used to find transaction patterns that are common and may be associated with fraud. An example is the following factors that are taken into account in the process of fraud detection: amount, time, place, type of product, payment method, user's location, etc. [12]. The disadvantage of the algorithm is the assumption that associative rules should be searched only on the set of patterns that are often used in fraud, which leads to the exclusion of important patterns that are rarely used.

Anomaly detection involves identifying transactions that deviate from normal user behaviour (unusual amounts, timeframes, geolocation, etc.). In addition, the relationships between different transaction variables are analysed (for example, between the type of product and the place of purchase) [13]. Such methods can have a significant level of first-order errors.

One way to solve this problem is to use a combined approach that combines different methods and allows for the detection of a wider range of fraud schemes and is more adaptable to new types of fraud. The combination of methods also helps to reduce the number of false classifications of legitimate transactions as fraud (first type errors) [14].

The aim of this paper is to improve the quality of payment fraud detection by implementing a combined approach to transaction analysis.

Developing a model for detecting fraud transactions

In this paper, the dataset used for the study is *creditcard.csv*, which contains transactions made with credit cards in September 2013 by European cardholders.

This dataset is transactions that occurred over a two-day period and contains 492 fraud cases out of 284,807 transactions. The dataset is highly unbalanced, with the positive class (fraud) accounting for 0.172% of all transactions. It contains only numeric input variables, which are the result of the PCA transformation. Due to confidentiality issues, the original names of the features and background information about the data are not available. The features V_1, V_2, … V_{28} are the principal components obtained by PCA; the only features not transformed by PCA are "time" and "amount". The "time" feature contains the seconds elapsed between each transaction and the first transaction in the dataset. The "amount" feature is the amount of the transaction, which can be used for training and cost consideration. The "class" function is a response variable that takes the value "1" if fraud is detected and "0" otherwise.

Preliminary analysis of the data showed no missing values and highly correlated features (over 90%). In addition, the data is unbalanced and requires balancing [15] or certain adjustments to the model parameters. After dividing the data into training and education sets, they were standardized and normalized.

In order to detect fraud transactions, the possibility of using classification models based on ensemble methods was investigated. To study their effectiveness, their software models were developed in the Colab Python environment. The models used as basic classifiers are XGBoost, SVC, Logistic Regression,

Сучасний стан наукових досліджень та технологій в промисловості. 2024. №4 (30)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

AdaBoostClassifier, K-Nearest Neighbors, and Isolation Forest. Gradient boosting algorithm (*XGBoost*) builds a model as an ensemble of decision trees. Each new tree adds information that was not taken into account by the previous trees. The Support Vector Classifier *(SVC)* builds a hyperplane that optimally divides the data into classes. Logistic Regression is a statistical method for predicting binary outcomes that calculates the probability that an object belongs to a certain class. The Adaptive Boosting algorithm is also an ensemble classifier that sequentially combines weak classifiers and combines them into a strong classifier. In this case, each new classifier is trained on data that was misclassified by previous classifiers. The misclassified objects receive more weight in subsequent iterations, and the final prediction is calculated as a weighted sum of the predictions of all weak classifiers. The K-Nearest Neighbors (*KNN*) algorithm classifies based on similarity. It assigns a new object to the class that is the most common among the k nearest neighbors of this object in the training set. The Isolation Forest algorithm is commonly used for anomaly detection. It builds isolation trees that recursively partition the data until each object is isolated. Each of these algorithms has its own advantages, which depend on the specific task and the source information. For example, the use of XGBoost and AdaBoost algorithms is effective for large datasets with complex relationships between features. *SVC* is productive when processing data with a nonlinear separation boundary. Logistic regression is easy to interpret and effective for binary classification. *KNN* does not require explicit model training, is easy to apply, but can be sensitive to noise. Isolation Forest is one of the most effective algorithms for anomaly detection.

Fig. 1 shows the results of binary classification quality for class "0" and class "1". To determine the quality of the model, we used the *f1-score*, which provides a balanced assessment of the model's performance, taking into account false positives and false negatives.

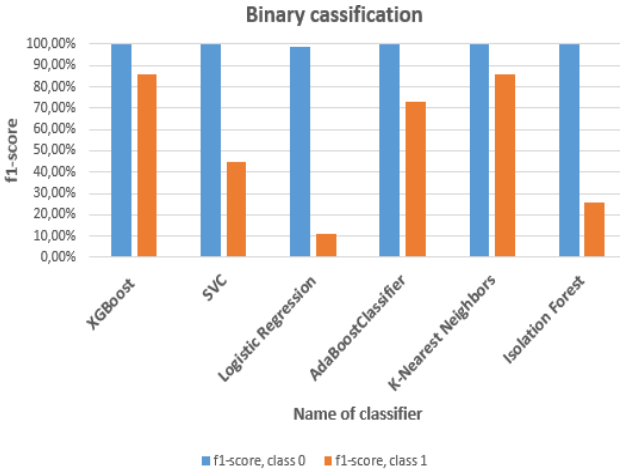

Fig. 1. Quality results of binary classification

As can be seen from fig. 1, the best results were achieved when using a model based on the gradient boosting algorithm. *XGBoost* belongs to the category of ensemble learning, in particular to the gradient boosting structure, uses decision trees as basic learning methods, and is known for its computational efficiency [16]. The model based on the gradient boosting algorithm also uses regularization methods to improve model generalization and is particularly effective in dealing with imbalanced data. For this purpose, the $scale\_pos\_weight$, tuning parameter is implemented to help balance the positive and negative classes by giving more weight to the minority class:

$$scale\_pos\_weight = \frac{Number\ of\ Positive Class\ Instances}{Number\ of\ Negative Class\ Instanses}.$$

The quality assessment of the model is shown in Fig. 2. As can be seen from the report, the model is biased towards the majority class, as the quality indicators for the majority class "0" are 100%. At the same time, the *f1-score* for the minority class is sufficient due to the increased weight of the minority class and amounts to 86%.

Classification Report for XGBoost:

	precision	recall	f1-score	support
0	1.00	1.00	1.00	56864
1	0.88	0.84	0.86	98
accuracy			1.00	56962
macro avg	0.94	0.92	0.93	56962
weighted avg	1.00	1.00	1.00	56962

Fig. 2. Classification Report

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)
Innovative technologies and scientific solutions for industries. 2024. No. 4 (30)

To improve the quality of fraud detection, we further clustered the labeled data. This approach is non-standard, but can be promising, providing new knowledge. In some cases, clustering divides the original classes into smaller subclasses. This can be useful for a more detailed analysis of the data, as the labeled data may contain hidden structures that were not taken into account during the labeling. Clustering can help to identify these structures and gain a deeper understanding of the data. It also helps to assess which features have the greatest impact on an object's belonging to a particular cluster.

The $(k\text{-}means)$ method is used for clustering. This method requires a predefined parameter k, the number of clusters. In the process of clustering by the $k\text{-}means$ method, the number of clusters is most often estimated using the elbow method. It involves repeatedly cycling through the algorithm, increasing the number of clusters to be selected, and then plotting the distortion score, defined as the sum of the squares of the intra-cluster distances to the cluster center $(WCSS, within\text{-}cluster\ sum\ of\ squares)$

$$WCSS = \sum_{C_k}^{C_n} \sum_{d_i in C_i}^{d_m} distance(d_i, C_k)^2,$$

where C – are the cluster centroids; d – are the data values in each cluster.

To select the optimal number of clusters, we used the KElbowVisualizer model of the Colab Python library with the distortion metric, which calculates the sum of the squares of the distances from each point to its designated center. The estimate of the optimal number of clusters is shown in fig. 3. The abscissa axis corresponds to the number of clusters, the ordinate axis to the distortion score and the model training time. In this case, the optimal number of clusters is the one that corresponds to the inflection point of the graph and minimizes the model training time. As can be seen from fig. 3, the optimal number of clusters is 12. That is, the original data can be divided into 12 subclasses.

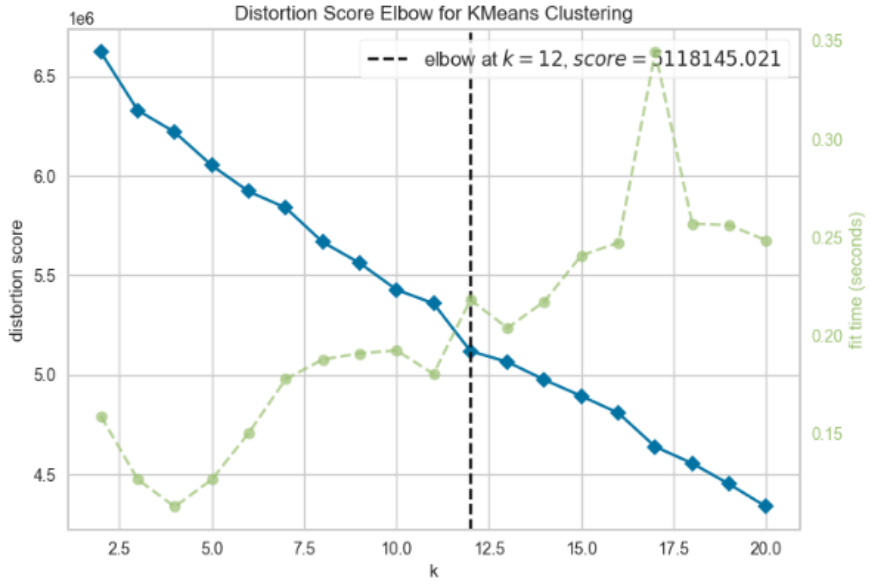

Fig. 3. Estimation of the optimal number of clusters

To build a multiclassification model for the newly labeled data, we used a model based on gradient boosting. Since the newly labeled data are also unbalanced, the *scale_pos_weight* parameter was reused in the process of model tuning. The results of multiclassification are shown in fig. 4.

The report shows that the quality of classification is excellent. The *F1-score* ranges from 96 to 100% for different subclasses.

The results are also confirmed by the ROC curve (fig. 5).

The next advantage of using gradient boosting is the ability to relatively easily obtain an information content score for each attribute. Features with high informativeness allow you to more accurately divide objects into classes and draw clearer boundaries between classes, which helps to improve classification accuracy. Selecting informative features helps to reduce data dimensionality, reduce noise, and increase model accuracy. Attribute informativeness also shows how useful or valuable each attribute was in building the

Сучасний стан наукових досліджень та технологій в промисловості. 2024. №4 (30)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

ensemble decision trees, which allows you to rank attributes and compare them with each other. In addition, attributes with low informativeness can be removed from the dataset, which is likely to speed up the speed of model training and testing.

Classification Report for XGBoost:

	precision	recall	f1-score	support
0	1.00	1.00	1.00	3294
1	0.99	0.99	0.99	2622
2	0.98	0.98	0.98	7607
3	0.99	0.99	0.99	11196
4	0.99	1.00	1.00	3942
5	0.98	0.98	0.98	341
6	0.98	0.99	0.98	9829
7	0.99	0.99	0.99	10417
8	0.96	0.97	0.96	721
9	0.97	0.96	0.97	621
10	1.00	1.00	1.00	6309
11	0.97	0.97	0.97	63
accuracy			0.99	56962
macro avg	0.98	0.98	0.98	56962
weighted avg	0.99	0.99	0.99	56962

Fig. 4. Results of multiclassification of source data by the *XGBoost* method

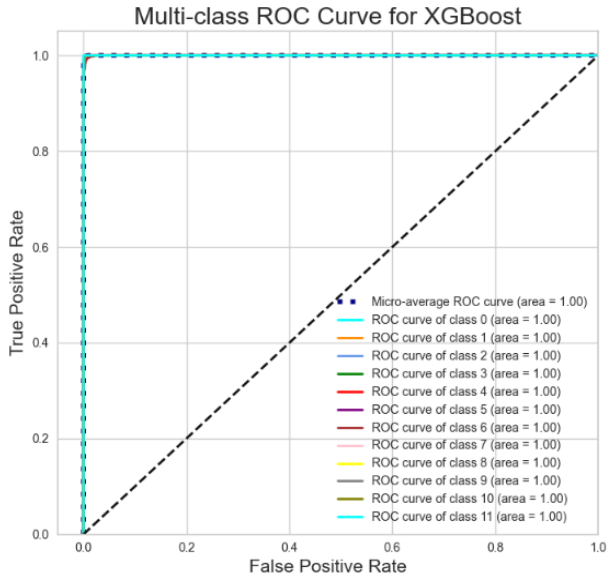

Fig. 5. *ROC* curve value as a result of multiclassification of the output data

The next advantage of using gradient boosting is the ability to relatively easily obtain an information content score for each attribute. Features with high informativeness allow you to more accurately divide objects into classes and draw clearer boundaries between classes, which helps to improve classification accuracy. Selecting informative features helps to reduce data dimensionality, reduce noise, and increase model accuracy. Attribute informativeness also shows how useful or valuable each attribute was in building the ensemble decision trees, which allows you to rank attributes and compare them with each other. In addition, attributes with low informativeness can be removed from the dataset, which is likely to speed up the speed of model training and testing.

Feature information is evaluated by the *feature_importances* attribute of the XGBClassifier model. In this case, for each tree, it is estimated how much all the features contribute to reducing the degree of chaos due to the distribution of data in the nodes of the decision tree. This evaluation criterion can be, for example, information entropy:

$$H = -\sum_{i=1}^{p} \frac{N_i}{N} \log_2 \left(\frac{N_i}{N} \right),$$

where n is the number of classes in the original subset; N_i is the number of objects of the i-th subclass; N is the total number of objects.

Subsequently, the importance of each feature for all trees is averaged to obtain the final indicator of its informativeness for the entire model.

First, we investigated the informativeness of the features before their clustering (Fig. 6). As can be seen from Fig. 6, the following features have the greatest impact on decision making: V_{12}, V_6, *Time*, V_{11}, V_{10}, V_{18}, V_{24}, *Amount*, V_2, V_{22}. Thus, the informativeness of the V_{12} feature is 11.61 %. That is, the value of this feature has the greatest impact on the object's belonging to the class of legitimate or fraud transactions.

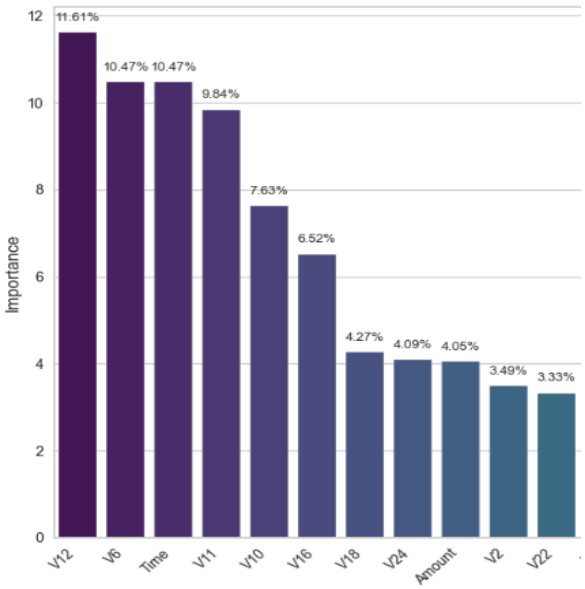

Fig. 6. Evaluation of the features informativeness before their clustering

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)
Innovative technologies and scientific solutions for industries. 2024. No. 4 (30)

Further research is related to the evaluation of the most informative features within each cluster (Figs. 7–9). To do this, the data is recursively divided into two classes – objects of the current cluster and other objects – and their informativeness is evaluated.

As can be seen from fig. 7, the following features are the most informative for the second cluster: V_3, V_{14}, V_4, V_7, *Amount*, etc.

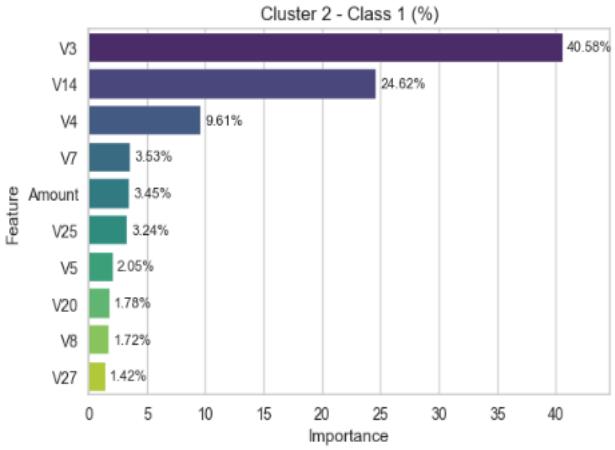

Fig. 7. Evaluation of the features informativeness for the second cluster

For the third cluster (fig. 8), the greatest influence on decision-making is provided by the features V_{10}, V_{12}, V_4, V_{14}, *Time*, V_8 etc.

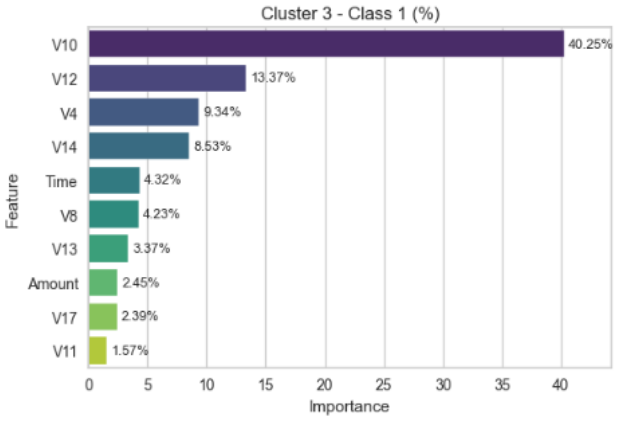

Fig. 8. Evaluation of the features informativeness for the third cluster

The analysis of fig. 9 shows that belonging to this cluster is determined by the *Amount* feature by 96.62%. That is, it can be assumed that the sequence of attributes by which objects were added to the eighth subclass allows you to access a bank account and withdraw all funds from the account at once in one transaction.

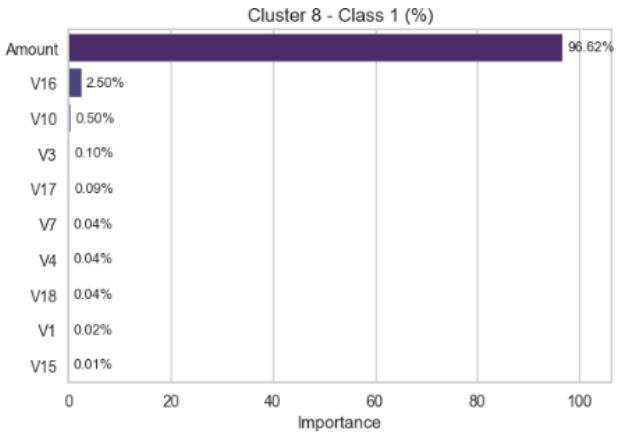

Fig. 9. Evaluation of the informativeness of features for the eighth cluster

Conclusions

The study analyzes various approaches to detecting fraud transactions. Methods based on data classification technology are considered and their software models are built in the Google Colab Python environment. The classifiers based on XGBoost, SVC, Logistic Regression, Logistic Regression, AdaBoostClassifier, K-Nearest Neighbors, Isolation Forest are investigated. The dataset used is *creditcard.csv*, which contains transactions made by European cardholders with credit cards in September 2013. This dataset is a two-day transaction and contains 492 fraud cases out of 284,807 transactions. Due to privacy concerns, the dataset is the result of a PCA transformation. There is no original feature name or background information about the data. The dataset is unbalanced. The best results are achieved by using a model based on gradient boosting. This model is particularly effective in dealing with unbalanced data because it contains a *scale_pos_weight* setting that helps to balance positive and negative classes by giving more weight to the minority class. It is determined that the *f1-score* due to the increase in the weight of the minority class is 86% for the minority class.

In order to improve the quality of fraud detection, we further cluster the labeled data. The *k-means* method was used for clustering. The number of clusters equal to 12 was determined by the elbow method. A model based on gradient boosting was used to build a multiclassification model for the newly labeled data. It was found that the quality of the model has improved significantly. The*F1-score* ranges from 96 to 100% for different subclasses.

Сучасний стан наукових досліджень та технологій в промисловості. 2024. №4 (30)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

Further, the informativeness of the features before and after their clustering was evaluated. To do this, we used the *feature_importances* attribute of the *XGBClassifier* model. The data are recursively divided into two classes – objects of the current cluster and other objects – and evaluated. It was found that within each subclass, the informativeness of the features is different. For example, belonging to the eighth cluster is 96.62% determined by the "amount" feature. That is, it is possible to assume that the sequence of attributes by which objects were added to the eighth subclass allows access to a bank account and withdraw all funds from the account simultaneously in one transaction.

Thus, the approach of combined use of data classification and clustering methods improves the quality of fraud transaction detection. The approach is useful for more detailed data analysis and identification of hidden structures that were not taken into account during the markup. It also helps to assess which features have the greatest impact on an object's belonging to a particular subclass.

References

1. Ivanna, Hordiichuk (2023), "V Ukraini zafiksovano anomalnu aktyvnist shakhraiv". available at: https://glavcom.ua/country/criminal/v-ukrajini-zafiksovano-anomalnu-aktivnist-shakhrajiv-959941.html
2. "U merezhi aktyvizuvalysia shakhrai, yaki proponuiut ukraintsiam «dopomohu» vid mizhnarodnykh orhanizatsii". available at: https://www.ukrinform.ua/rubric-society/3702800-u-merezi-aktivizuvalisa-sahrai-aki-proponuut-ukraincam-dopomogu-vid-miznarodnih-organizacij.html
3. Viktoriia, Telechuk "U Facebook diie fishynhova skhema shakhraistva: yak vberehtysia". available at: https://rayon.in.ua/news/575310-u-facebook-die-fishingova-skhema-shakhraystva-yak-vberegtisya
4. Voinarska, I. A. (2021), "Shakhraistvo u nerukhomosti, Ekonomika. Finansy". Pravo. № 4. P. 31–32. available at: http://nbuv.gov.ua/UJRN/ecfipr_2021_4_8
5. "Kartkovi shakhrai hrabuiut ukraintsiv sylnishe: yaki skhemy vynakhodiat i yak zakhystytysia" (2024). available at: https://minfin.com.ua/ua/credits/articles/kartochnye-moshenniki-grabyat-ukraincev-silnee-kakie-shemy-izobretayut-i-kak-zaschititsya/
6. Kaprian, Yu. (2023), "Vykorystannia mashynnoho navchannia dlia borotby z bankivskym shakhraistvom", Biznes Inform. № 7. P. 140–145. available at: https://www.businessinform.net/_inc/kachka_pdf.php?year=2023&volume=7_0&pages=140_145&qu=%D1%88%D0%B0%D1%85%D1%80%D0%B0%D0%B
7. Sinha, A. and Mokha, S. (2017), "Classification and fraud detection in finance industry ", *International Journal of Computer Applications*, Vol. 176, no. 3, P. 45–52. DOI: https://doi.org/10.5120/ijca2017915570
8. Gavrylenko , S., Poltoratskyi , V., & Nechyporenko , A. (2024), "Intrusion detection model based on improved transformer", *Advanced Information Systems*, 8(1), P. 94–99. DOI: https://doi.org/10.20998/2522-9052.2024.1.12
9. Gavrylenko, S., Chelak, V., Hornostal O. (2021), "Ensemble approach based on bagging and boosting for Identification the Computer System State", *Proceedings of the 31th International Scientific Symposium Metrology and Metrology Assurance (MMA)*.Sozopol, Bulgaria, P. 1–7. available at: https://ieeexplore.ieee.org/document/9610949
10. Lepoivre, M. (2016), "Credit Card Fraud Detection with Unsupervised Algorithms", *Journal of Advances in Information Technology*, Vol. 7, no. 1. P. 34–38. DOI: https://doi.org/10.12720/jait.7.1.34-38
11. Leonard, K. (1993), "Detecting credit card fraud using expert systems", *Computers & Industrial Engineering*. 1993. Vol. 25, no. 1-4. P. 103–106. DOI: https://doi.org/10.1016/0360-8352(93)90231-l
12. Abhishek, A. (2021), "Predictive Analytics with Machine Learning for Fraud Detection", *International Journal for Research in Applied Science and Engineering Technology*, Vol. 9, no. 11. P. 1518–1520. DOI: https://doi.org/10.22214/ijraset.2021.39046
13. Vanarote, V. (2021), "Transaction Fraud Detection (Anomaly detection) using Machine Learning", *International Journal of Advanced Research in Science, Communication and Technology*, P. 361–363. DOI: https://doi.org/10.48175/ijarsct-1402
14. Nadisha, A., Rakendu R, Surekha M. (2015), "A Hybrid Approach to Detect Credit Card Fraud", *International Journal of Scientific and Research Publications*, Vol. 5, Issue 11, P. 304–314. available at: https://www.ijsrp.org/research-paper-1115.php?rp=P474793
15. Gavrylenko, S., Zozulia, V., and Khatsko, N. (2023), "Methods for Improving the Quality of Classification on Imbalanced Data", *Proceedings of the IEEE 4th KhPI Week on Advanced Technology (KhPIWeek)*, Kharkiv, Ukraine, P. 1–5. DOI: https://doi.org/10.20998/2522-9052.2024.1.12

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) *Innovative technologies and scientific solutions for industries. 2024. No. 4 (30)*

16. Hajek, P, Abedin M., Sivarajah, U. (2022), "Fraud Detection in Mobile Payment Systems using an XGBoost-based Framework", *Inf Syst Front*, P. 1–19. DOI: https://doi.org/10.1007/s10796-022-10346-6

Надійшла (Received) 03.11.24

Відомості про авторів / About the Authors

Гавриленко Світлана Юріївна – доктор технічних наук, професорка, Національний технічний університет "Харківський політехнічний інститут", професорка кафедри "Комп'ютерна інженерія та програмування", Харків, Україна; e-mail: gavrilenko08@gmail.com; ORCID ID: https:// orcid.org/ 0000-0002-6919-0055

Абдуллін Олексій Ренатович – Національний технічний університет "Харківський політехнічний інститут", магістр, Харків, Україна; e-mail: drftg4@gmail.com; ORCID ID: https://orcid.org/0009-0007-8799-4253

Gavrylenko Svitlana – Doctor of Sciences (Engineering), Professor, National Technical University "Kharkiv Polytechnic Institute", Professor at the Department of "Computer Engineering and Programming", Kharkiv, Ukraine.

Abdullin Oleksii – National Technical University "Kharkiv Polytechnic Institute", Master, Kharkiv, Ukraine.

ПІДВИЩЕННЯ ЯКОСТІ ВИЯВЛЕННЯ ПЛАТІЖНОГО ШАХРАЙСТВА ВНАСЛІДОК ВИКОРИСТАННЯ КОМБІНОВАНОГО ПІДХОДУ АНАЛІЗУ ТРАНЗАКЦІЙ

Предмет дослідження – методи виявлення шахрайських транзакцій. **Метою роботи** є підвищення якості виявлення платіжного шахрайства за допомогою використання комбінованого підходу аналізу транзакцій. **Завдання**: дослідити методи виявлення шахрайських транзакцій та запропонувати підхід для підвищення якості їх виявлення. **Методи**: штучний інтелект, машинне навчання. **Досягнуті результати.** Досліджено методи виявлення шахрайських транзакцій; розглянуто методи, основані на технології класифікації даних, зокрема *XGBoost, SVC, Logistic Regression, Logistic Regression, AdaBoostClassifier, K-Nearest Neighbors, Isolation Forest,* та побудовано їх програмні моделі. Як вихідних дані застосовано набір *creditcard.csv*, що містить транзакції, здійснені європейськими власниками карток, які відбулися за два дні, та містить 492 випадки шахрайства з 284807 транзакцій. Найкращий результат досягнутий унаслідок використання моделі на основі градієнтного бустингу, яка дає змогу обробляти незбалансовані дані. Виявлено, що *f1-score* за допомогою застосування параметра ваги класу меншості становить 86% для міноритарного класу. З метою підвищення якості виявлення шахрайства виконано кластеризацію розмічених даних на підкласи із використанням методу *k*-середніх. Кількість кластерів, що дорівнює 12, визначено методом "ліктя". Це дало змогу підвищити якість мультикласифікації. З'ясовано, що якість моделі значно покращилась. *F1-score* становить від 96 до 100% для різних підкласів. Оцінено інформативності ознак у межах кожного підкласу алгоритмом градієнтного бустингу. Результати експерименту показали різний вплив ознак на належність до підкласу, що дає змогу більш детально проаналізувати дані з метою виявлення в них прихованих структур. **Висновки**. Наукова новизна досягнутих результатів полягає в комбінованому використанні методів класифікації та кластеризації даних для виявлення шахрайських транзакцій, що дало змогу зменшити кількість помилок другого роду. Оцінювання інформативності ознак у межах різних типів (підкласів) шахрайських транзакцій допомагає визначити, які ознаки найбільше впливають на належність об'єкта до того чи іншого підкласу.

Ключові слова: машинне навчання; шахрайські транзакції; класифікація; кластеризація; інформативність ознак.

Бібліографічні описи / Bibliographic descriptions

Гавриленко С. Ю., Абдулов О. Р. Підвищення якості виявлення платіжного шахрайства внаслідок використання комбінованого підходу аналізу транзакцій. *Сучасний стан наукових досліджень та технологій в промисловості*. 2024. № 4 (30). С. 31–38. DOI: https://doi.org/10.30837/2522-9818.2024.4.031

Gavrylenko, S., Abdulov, O. (2024), "Improving the quality of payment fraud detection by using a combined approach of transaction analysis", *Innovative Technologies and Scientific Solutions for Industries*, No. 4 (30), P. 31–38. DOI: https://doi.org/10.30837/2522-9818.2024.4.031