UDC 65.011 DOI https://doi.org/10.35546/kntu2078-4481.2025.3.2.23

O. A. YEROSHENKO
Doctor of Philosophy,
Associate Professor a the Department of Electronic Computers
Kharkiv National University of Radio Electronics
ORCID: 0000-0001-6221-7158

A. I. ANDRUSHCHENKO
Student at the Department of Electronic Computers
Kharkiv National University of Radio Electronics
ORCID: 0009-0001-5179-5611

A. R. SOROKIN
Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Department of Electronic Computers
Kharkiv National University of Radio Electronics
ORCID: 0000-0002-4383-2611

V. I. SITNIKOV
Assistant at the Department of Electronic Computers
Kharkiv National University of Radio Electronics
ORCID: 0009-0005-3087-6104

APPLICATION OF ENSEMBLE LEARNING ALGORITHMS FOR FRAUD DETECTION IN BANKING TRANSACTIONS

This paper examines the use of ensemble machine learning methods for detecting and preventing banking fraud, which today represents one of the key threats to financial stability and the security of clients of financial institutions. The rapid development of digital technologies creates both new opportunities for optimizing financial processes and new challenges associated with increasingly sophisticated fraud schemes. In this regard, the task of detecting suspicious transactions requires high-tech and reliable solutions.

The proposed approach involves the use of an ensemble model that combines the results of several machine learning algorithms, which helps to compensate for the weaknesses of individual models and provide more stable classification. Special attention is given to preliminary data preprocessing: normalization, class balancing, and the selection of the most informative features that directly influence model accuracy. One of the key requirements of the study is to reduce the number of fraudulent transactions that may be incorrectly classified as legitimate, since such cases not only cause financial losses for the bank but also harm its reputation and customer trust.

Within the study, a comparative analysis of the ensemble method and single machine learning models was conducted, identifying the advantages and disadvantages of the proposed solution. The choice of this approach is also driven by its high practicality, compatibility with financial systems, and ease of integration. The ensemble method makes it possible to combine the strengths of simple models while reducing the impact of their weaknesses on the final result. Overall, the choice of software should depend on the project's technical requirements, and to achieve the best results, different models and approaches should be analyzed. The results confirm that the use of ensemble methods increases classification accuracy and reduces the likelihood of false positives. This makes the proposed approach a promising tool for enhancing the protection of banking institutions against fraud and minimizing financial risks.

Key words: *banking fraud, classification, random forest, linear regression, decision tree, neural networks.*

О. А. ЄРОШЕНКО
доктор філософії,
доцент кафедри електронних обчислювальних машин
Харківський національний університет радіоелектроніки
ORCID: 0000-0001-6221-7158

© Yeroshenko O. A., Andrushchenko A. I., Sorokin A. R., Sitnikov V. I., 2025
Стаття поширюється на умовах ліцензії CC BY 4.0

А. І. АНДРУЩЕНКО
здобувач кафедри електронних обчислювальних машин
Харківський національний університет радіоелектроніки
ORCID: 0009-0001-5179-5611

А. Р. СОРОКІН
кадидат технічних наук, доцент,
доцент кафедри електронних обчислювальних машин
Харківський національний університет радіоелектроніки
ORCID: 0000-0002-4383-2611

В. І. СІТНІКОВ
асистент кафедри електронних обчислювальних машин
Харківський національний університет радіоелектроніки
ORCID: 0009-0005-3087-6104

ЗАСТОСУВАННЯ АЛГОРИТМІВ АНСАМБЛЕВОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ ШАХРАЙСТВА В БАНКІВСЬКИХ ТРАНЗАКЦІЯХ

У роботі розглянуто застосування ансамблевих методів машинного навчання для виявлення та запобігання банківському шахрайству, яке сьогодні є однією з ключових загроз фінансовій стабільності та безпеці клієнтів фінансових установ. Швидкий розвиток цифрових технологій створює як нові можливості для оптимізації фінансових процесів, так і нові виклики, пов'язані з появою більш складних схем шахрайства. З огляду на це, завдання виявлення підозрілих транзакцій потребує високотехнологічних і надійних рішень.

Запропонований підхід передбачає використання ансамблевої моделі, яка поєднує результати роботи кількох алгоритмів машинного навчання, що дозволяє компенсувати недоліки окремих моделей і забезпечити більш стабільну класифікацію. Особливу увагу приділено попередньому препроцесингу даних: виконано нормалізацію, балансування класів та вибір найбільш інформативних ознак, що безпосередньо впливають на точність моделі. Однією з ключових вимог дослідження є зменшення кількості шахрайських транзакцій, які можуть бути помилково класифіковані як легітимні, адже такі випадки завдають не лише фінансових збитків банку, а й шкодять його репутації та довірі клієнтів.

У межах дослідження проведено порівняльний аналіз ансамблевого методу та одиночних моделей машинного навчання, визначено переваги та недоліки запропонованого рішення. Вибір даного підходу зумовлений також високою практичністю, сумісністю з фінансовими системами а також простотою інтеграції. Ансамблевий метод допомагає поєднати переваги простих моделей та зменшити вплив їхніх недоліків на кінцевий результат. В загальному, вибір програмного забезпечення повинен залежати від технічних вимог проекту і для отримання кращих результатів слід аналізувати різні моделі та підходи. Результати підтверджують, що використання ансамблевих методів забезпечує підвищення точності класифікації та зниження ймовірності помилкових спрацювань. Це робить запропонований підхід перспективним інструментом для підвищення рівня захисту банківських установ від шахрайства та мінімізації фінансових ризиків.

Ключові слова: *банківське шахрайство, класифікація, випадковий ліс, лінійна регресія, дерево рішень, нейронні мережі.*

Problem Statement

The volume of banking transactions conducted electronically, including through internet banking and mobile applications, is growing every year. Along with this, the number of fraudulent activities is also increasing, leading to significant financial losses for both banking institutions and their clients. According to international studies, annual losses from fraudulent operations in the banking sector amount to billions of dollars.

The problem is complicated by several factors. User behavior is highly variable: transactions may differ in amount, time, geographical location, and method of execution. This natural variability makes it difficult to establish clear criteria to distinguish legitimate operations from fraudulent ones. Fraudsters actively exploit modern technologies, using stolen or fabricated credentials, phishing schemes, identity theft, automated bots for large-scale attacks, and methods of concealing traces (such as IP spoofing or the use of VPNs). This forces security systems to constantly adapt to new attack scenarios. In typical datasets, fraudulent transactions usually account for less than 1 % of the total volume, resulting in a severe class imbalance. Under such conditions, standard machine learning algorithms often prove ineffective, as they tend to ignore the minority yet most critical class [1–2].

Modern approaches to fraud detection in financial transactions largely rely on machine learning methods. These methods can analyze large amounts of data, identify hidden patterns, and generate predictions based on complex multidimensional dependencies. However, the use of traditional models, such as logistic regression or classical decision trees, has limitations. They often demonstrate insufficient generalization ability and are not always effective in detecting

complex or atypical fraud scenarios. Another issue is the large number of false positives, where the system incorrectly classifies legitimate transactions as fraudulent. This not only creates additional workload for the bank's security services but also negatively affects the customer experience, as legitimate users face blocked or delayed transactions [3–4].

In this context, ensemble learning methods, which combine the results of multiple models, represent a promising direction. They improve anomaly detection efficiency by reducing the impact of random errors and generalizing information from different sources. Moreover, methods such as Random Forest, Gradient Boosting, and Extreme Gradient Boosting offer high flexibility and accuracy in identifying complex patterns, which is crucial in combating fraud. The application of these methods makes it possible not only to reduce the number of false results but also to adapt models to changes in user behavior and evolving fraud schemes [5–6].

The study of ensemble machine learning methods in fraud detection is both relevant and practically significant. It combines scientific interest, associated with the development of new models and approaches to big data analysis, with applied value for financial institutions seeking to minimize risks and strengthen customer trust in their services. This paper explores modern approaches to fraud detection, analyzes the specifics of using ensemble algorithms, and demonstrates their potential for improving the accuracy and reliability of financial security systems.

Analysis of Recent Studies and Publications

In works [7], methods of applying machine learning algorithms for fraud detection are described. In particular, the use of decision trees is considered, which provide basic efficiency but face limitations in cases of complex data patterns. The advantages of ensemble methods, such as Random Forest and Gradient Boosting, which demonstrate higher accuracy in classification tasks, are also analyzed in detail. Works [8] focus on the application of deep learning methods, which, although yielding good results, require significant computational resources and training time.

Despite the progress in this field, several issues remain unresolved. These include the optimal tuning of ensemble models, the selection of the most effective algorithms in the context of fraud detection, and the analysis of their resilience to changes in user behavior patterns. Particularly relevant is the development of approaches that ensure a balance between accuracy and real-time transaction processing speed, since delays in the financial sector may have critical consequences for both clients and banking institutions.

Formulation of the Research Objective

The objective of the study is to develop and substantiate an effective model for detecting fraudulent transactions in the banking sector through the application of ensemble machine learning methods. These methods are intended to increase classification accuracy and reduce the number of misclassified operations, while taking into account business requirements and the practical aspects of integration into financial systems.

Presentation of the Main Research Material

Ensemble learning methods are a powerful tool in classification and regression tasks. For fraud detection, the most effective algorithms are Random Forest, Gradient Boosting, AdaBoost, and Extreme Gradient Boosting. These methods combine the results of several base models, which reduces the impact of random errors and improves prediction accuracy. An important aspect of these methods is their ability to account for different types of dependencies within the data, which enhances their flexibility in complex tasks such as fraud detection.

Random Forest is known for its resistance to overfitting due to the use of random feature and data sampling when constructing each tree in the ensemble. Gradient Boosting, in turn, seeks to minimize the errors of previous models through sequential learning. Extreme Gradient Boosting, as an improved version of Gradient Boosting, ensures optimization of speed and performance through computational enhancements and regularization. AdaBoost focuses on correcting the errors of previous base models by assigning higher weights to difficult-to-classify samples. This feature makes it effective when working with data that exhibits high variability or anomalies.

In this study, data closely approximating real banking transactions with labeled fraudulent and legitimate operations were used. Preliminary data analysis included the removal of missing values to prevent their impact on modeling results. Normalization of values helped to reduce the influence of variable scales, while encoding categorical variables using the "one-hot encoding" method ensured the proper handling of non-numeric data.

In this research, the following formulas were used to evaluate the effectiveness of machine learning models in detecting fraud in banking transactions:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN};$$

$$\text{Recall} = \frac{TP}{TP + FN};$$

$$\text{Precision} = \frac{TP}{TP + FP};$$

$$\text{Fl} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}},$$

where TP – true positives (correctly identified fraudulent transactions), TN – true negatives (correctly identified legitimate transactions), FP – false positives (legitimate transactions incorrectly classified as fraudulent), FN – false negatives (fraudulent transactions that remain undetected).

Correlation analysis helped to identify the most significant variables for modeling, which improved the efficiency of model training. Particular attention was paid to reducing class imbalance, which is typical for fraud detection tasks. To address this, the SMOTE (Synthetic Minority Over-sampling Technique) method was applied, generating additional synthetic samples for the minority class of fraudulent transactions. This significantly improved model performance, especially in Recall and F1-score metrics, which are critically important for fraud detection tasks.

The experimental analysis demonstrated that combining ensemble learning methods with modern data preprocessing techniques allows achieving high levels of Accuracy, Recall, and Precision. Moreover, the models showed robustness to new types of data that were not used during training.

Fraud detection in transactions involves data collection, preprocessing, model selection and tuning, as well as evaluation and deployment. Data should be collected from various sources, such as banking transactions, log files, customer information, and purchase history. These data must include timestamps, transaction amounts, transaction locations, types of operations, as well as payer and recipient information. This may require access to internal databases.

A key step is preprocessing the collected datasets. It is necessary to remove duplicates, handle missing values, and eliminate anomalies. Afterward, the data should be normalized and, if needed, clustered. Categorical variables must be encoded into numerical values. The creation of new informative features can significantly enhance model performance. At the same time, it is important to select the most relevant features. New features may include, for example, the average transaction amount or the number of transactions performed by a particular user within a day or another time period.

Fraudulent transactions usually account for less than 1 % of total payments, leading to imbalance in the collected datasets. Working with such data may be ineffective. This issue can be addressed through resampling methods, such as oversampling (e.g., SMOTE) or undersampling. After this, an appropriate method must be chosen to build a machine learning model. Since the task is a classification problem, possible approaches include logistic regression, decision trees, Random Forest, Gradient Boosting, and deep learning. Each of these models has its advantages and disadvantages, and the final choice depends on the specific requirements and conditions.

Once the model has been trained, it should be evaluated using relevant metrics. The main metrics include Accuracy, Recall, Precision, F1-score, and ROC-AUC. These metrics help assess how well the model detects fraudulent transactions and distinguishes them from legitimate ones [7].

Logistic regression is the most common method for solving classification problems, including fraud detection in transactions. It is based on modeling the probability of an object belonging to one of two classes using a linear combination of input features. Logistic regression employs a sigmoid function to transform the linear combination of features into the probability that a transaction is fraudulent.

In the course of the study, ensemble methods Random Forest, Gradient Boosting, XGBoost, and AdaBoost were built and tested for the task of detecting fraudulent transactions. The data were preprocessed by cleaning, normalizing, encoding categorical variables, and balancing classes using SMOTE, which significantly improved the results.

Table 1

Table of Research Results

Model	Accuracy	Precision	Recall	F1-score	ROC-AUC
Random Forest	0.9995	0.9610	0.7551	0.8457	0.9580
Gradient Boosting	0.9993	0.9100	0.8015	0.8522	0.9642
XGBoost	0.99954	0.8830	0.8469	0.8646	0.9691
AdaBoost	0.9989	0.8702	0.7024	0.7762	0.9427

The ROC curve is a graphical representation of the performance of a classification model at different decision thresholds. It shows the relationship between the True Positive Rate (TPR, or Recall) and the False Positive Rate (FPR).

The graph displays ROC curves for all models. XGBoost has the highest AUC score (0.9691), indicating the best ability to distinguish fraudulent transactions from legitimate ones. Gradient Boosting (0.9642) shows results close to XGBoost. Random Forest (0.9580) also demonstrates strong classification performance. AdaBoost (0.9427), however, lags behind the others, having the lowest AUC value.

The confusion matrices provide insights into the real-world performance of the models on positive (fraudulent) and negative (legitimate) transactions. Random Forest achieves the highest Precision (0.9610), meaning it produces the fewest false positives. However, its Recall (0.7551) is lower, so some fraudulent transactions remain undetected. Gradient Boosting delivers a higher Recall (0.8015) compared to Random Forest, but its Precision (0.9100) is slightly reduced. This results in a greater proportion of fraud detection but also an increase in false alarms. XGBoost provides the best balance between Precision and Recall, with the highest Recall (0.8469) and the highest F1-score (0.8646), making it the

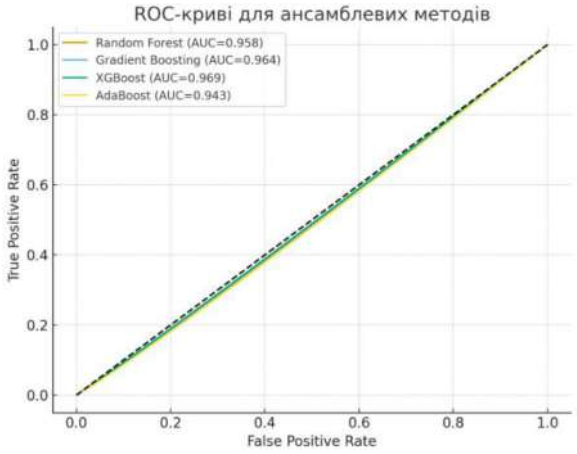

Fig. 1. ROC Curve for Ensemble Methods

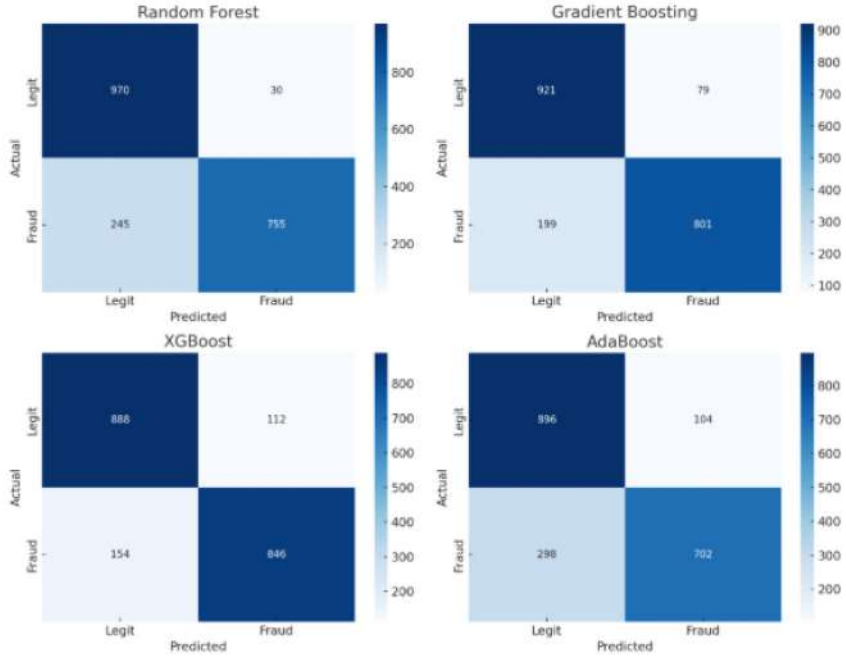

Fig. 2. Confusion Matrix for Ensemble Models

most effective for practical use. AdaBoost performs the weakest among the models: its Recall (0.7024) is the lowest, and although its Precision (0.8702) is acceptable, the overall F1-score is significantly lower.

In this section, the performance of classification models was analyzed using the ROC curve and the Confusion Matrix. The obtained results demonstrate that the models are capable of effectively separating fraudulent transactions from legitimate ones while maintaining balanced levels of accuracy and sensitivity. This confirms the feasibility of applying such models for fraud detection tasks in financial systems.

Conclusions

The conducted study confirmed the effectiveness of applying ensemble machine learning methods to the task of fraud detection in banking transactions. The use of algorithms such as Random Forest, Gradient Boosting, Extreme Gradient Boosting, and AdaBoost made it possible to achieve high levels of accuracy, sensitivity, and specificity. These models demonstrated the ability to effectively identify complex patterns in data, reduce the impact of random errors, and ensure reliable results under various conditions. Particularly important is the significant reduction in false positives, which increases customer trust in banking services and allows financial institutions to focus on genuine threats.

A substantial contribution to the research results was made by the integration of modern data preprocessing techniques. In particular, handling missing values, value normalization, categorical variable encoding using one-hot encoding, and applying SMOTE for class balancing improved the quality of model training. These approaches enabled the consideration of real-world data characteristics, such as class imbalance and high variability. The successful combination of data

preprocessing with ensemble algorithms resulted in robust models capable of performing effectively even on large and complex datasets.

The scientific novelty of the research lies in its comprehensive approach to the analysis and optimization of ensemble methods for fraud detection. Specifically, combining various ensemble learning algorithms with advanced preprocessing techniques allowed for the achievement of new results, which can serve as a foundation for further studies in this field. Additionally, the research demonstrated the high effectiveness of machine learning methods in detecting complex anomalies in data, making the findings applicable to a wide range of tasks.

The practical significance of this work lies in the potential to implement the proposed approaches to enhance the efficiency of existing banking transaction monitoring systems. In particular, the research results can be used to develop automated fraud detection systems capable of operating in real time while maintaining high accuracy and processing speed. Beyond the financial sector, the approaches developed in this study can be adapted to other industries, such as insurance, e-commerce, and telecommunications, where effective anomaly detection is crucial.

The results obtained highlight the promising potential of further research into ensemble methods and their integration with new data analysis techniques, which will further improve the effectiveness of fraud detection systems and related applications.

Bibliography

1. Almarshad F. A., Gashgari G. A., Alzahrani A. I. A. Generative adversarial networks-based novel approach for fraud detection for the European cardholders 2013 dataset. *IEEE Access*. Vol. 11. 2023. Pp. 107348–107368.

2. Hancock J. T., Bauder R. A., Wang H., Khoshgoftaar T. M. Explainable machine learning models for Medicare fraud detection. *Journal of Big Data*. Vol. 10, no. 1. 2023.

3. Alsayaydeh J. A. J., Aziz A., Rahman A. I. A. Development of programmable home security using GSM system for early prevention. *ARPN Journal of Engineering and Applied Sciences*. Vol. 16, no. 1. 2021. Pp. 88–97.

4. Fedorchenko I., Oliinyk A., Alsayaydeh J. A. J. Modified genetic algorithm to determine the location of the distribution power supply networks in the city. *ARPN Journal of Engineering and Applied Sciences*. Vol.15, no. 23. 2020. Pp. 2850–2867.

5. Shakhovska N., Liaskovsky D., Augousti A., Liaskovska S., Martyn Y. Design and deployment of data developer toolkit in cloud manufacturing environments. *CEUR-WS*. Vol. 3699. 2024. Pp. 47–56.

6. Fedorchenko V., Yeroshenko O., Shmatko O., Kolomiitsev O., Omarov M. (2024) Password hashing methods and algorithms on the.Net platform, *Advanced Information Systems*. Vol. 8, no. 4. 2024. Pp. 82–92.

7. Islam M. A., Uddin M. A., Aryal S., Stea G. An ensemble learning approach for anomaly detection in credit card data with imbalanced and overlapped classes. *Journal of Information Security and Applications*. Vol. 78. 2023.

8. Abdul Salam M., Fouad K. M., Elbably D. L., Elsayed S. M. Federated learning model for credit card fraud detection with data balancing techniques. *Neural Computing and Applications*. Vol. 36, no. 11. 2024. Pp. 6231–6256.

References

1. Almarshad, F. A., Gashgari, G. A., Alzahrani, A. I. A. (2023). Generative adversarial networks-based novel approach for fraud detection for the European cardholders 2013 dataset. *IEEE Access*. vol. 11, pp. 107348–107368.

2. Hancock, J. T., Bauder, R. A., Wang, H., Khoshgoftaar, T. M. (2023). Explainable machine learning models for Medicare fraud detection. *Journal of Big Data*. vol. 10, no. 1.

3. Alsayaydeh, J. A. J., Aziz, A., Rahman, A. I. A., et al. (2021). Development of programmable home security using GSM system for early prevention. *ARPN Journal of Engineering and Applied Sciences*. vol. 16, no. 1, pp. 88–97.

4. Fedorchenko, I., Oliinyk, A., Alsayaydeh, J. A. J., et al. (2020). Modified genetic algorithm to determine the location of the distribution power supply networks in the city. *ARPN Journal of Engineering and Applied Sciences*. Vol. 15, no. 23, pp. 2850–2867.

5. Shakhovska, N., Liaskovsky, D., Augousti, A., Liaskovska, S., Martyn, Y. (2024). Design and deployment of data developer toolkit in cloud manufacturing environments. *CEUR-WS*. vol. 3699, pp. 47–56.

6. Fedorchenko, V., Yeroshenko, O., Shmatko, O., Kolomiitsev, O., Omarov, M. (2024) Password hashing methods and algorithms on the.Net platform, *Advanced Information Systems*, vol. 8, no. 4, pp. 82–92.

7. Islam, M. A., Uddin, M. A., Aryal, S., Stea, G. (2023). An ensemble learning approach for anomaly detection in credit card data with imbalanced and overlapped classes. *Journal of Information Security and Applications*. vol. 78.

8. Abdul Salam, M., Fouad, K. M., Elbably, D. L., Elsayed, S. M. (2024). Federated learning model for credit card fraud detection with data balancing techniques. *Neural Computing and Applications*. vol. 36, no. 11, pp. 6231–6256.

Дата першого надходження рукопису до видання: 21.09.2025
Дата прийнятого до друку рукопису після рецензування: 17.10.2025
Дата публікації: 28.11.2025