УДК 004.46

Горпініч І.О., студ. гр. КНТ-215м, магістрант,
Зайко Т.А., к.т.н, доцент
Національний університет «Запорізька політехніка»

ІНТЕЛЛЕКТУАЛЬНІ МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТРАНЗАКЦІЙНИХ ДАНИХ ТА ВИЯВЛЕННЯ ШАХРАЙСТВА

У сучасному світі фінансові транзакції стають дедалі більш цифровими, що призводить до збільшення ризику шахрайських операцій. Виявлення шахрайства є критично важливим для банків та платіжних систем, оскільки шахрайські транзакції призводять до значних фінансових збитків. Класичні методи аналізу, засновані на правилах або статичних моделях, не завжди ефективні через велике розбалансування класів та високу динамічність шахрайських схем. Використання методів штучного інтелекту та глибокого навчання дозволяє автоматично виявляти аномалії та прогнозувати ризик шахрайства з високою точністю [1].

Метою роботи є створення моделі для класифікації транзакцій на нормальні та шахрайські з використанням гібридного підходу, який поєднує можливості автоенкодера [2]-[3] та нейронного класифікатора, а також аномалійно-детекційного методу Isolation Forest [4]–[5]. Використана вибірка Credit Card Fraud Detection [6], яка містить числові ознаки транзакцій та мітки класів.

Основними проблемами було те, що:

- клас шахрайських транзакцій становить приблизно 0.2% від усіх даних;
- модель повинна виявляти аномалії навіть у разі обмежених даних для тренування.

В роботі запропоновано гібридну модель Hybrid Deep Autoencoder Isolation Fraud Detection [7]:

- autoencoder [2]-[3] призначений для навчання компактного представлення нормальних транзакцій. Вхідний вектор приймає 64 нейрони в латентному просторі міститься 16 нейронів в кінці реконструкція вхідних даних. Різниця між вхідними даними та реконструкцією використовується як ознака аномалії;
- нейронний класифікатор (Classifier) приймає латентне представлення та reconstruction error. Складається з одного прихованого шару з 32 нейронами та Dropout для запобігання перенавчанню;

- isolation forest [4]-[5] використовується для оцінки ймовірності аномалії на основі дерева рішень. Додає інформацію про нетипові транзакції для фінальної оцінки;
- фінальна оцінка транзакції обчислюється як середнє значення ймовірності від нейронної мережі та аномальної оцінки Isolation Forest. Порогове значення 0.3, що оптимізовано для балансу precision та recall шахрайських транзакцій.

Модель навчалася 30 епох із використанням оптимізатора Adam та комбінації BCEWithLogitsLoss для класифікації та MSELoss для reconstruction error. В табл.1 представлено результати отримані на тестовій вибірці.

Таблиця 1

Результати на тестовій вибірці

Клас	Precision	Recall	F1-score	Support
Normal(0)	0.86	0.99	0.92	394
Fraud(1)	0.91	0.33	0.48	98

Загальні метрики accuracy 0.86, roc-auc 0.923 [8].

Високий roc-auc 0.92 підтверджує, що модель ефективно відокремлює шахрайські транзакції. Precision шахрайських транзакцій 0.91 означає, що більшість передбачених шахрайських операцій справді є шахрайськими. Recall [8] 0.33 можна покращити за рахунок адаптивного порогу для конкретних бізнес-завдань.

Запропонований гібридний підхід поєднує автоенкодер, нейронний класифікатор та Isolation Forest, що дозволяє ефективно виявляти аномалії та шахрайство.

Використання reconstruction error у поєднанні з латентним представленням покращує розпізнавання складних шаблонів шахрайських транзакцій.

Модель показала високий ROC-AUC [8] 0.92, що свідчить про ефективність алгоритму навіть при сильно розбалансованих даних.

Для практичного застосування можна регулювати поріг класифікації 0.3 – 0.5 для балансування precision та recall залежно від фінансових ризиків.

Список використаних джерел:

1 Nasteski V. An overview of the supervised machine learning methods 2017. Vol. 4, №. 51-62. P. 56. URL: https://www.researchgate.net/profile/Vladimir-Nasteski/publication/328146111_An_overview_of_the_supervised_machine_learning_methods/links/5c1025194585157ac1bba147/An-overview-of-the-supervised-machine-learning-methods.pdf

2 Misra S. et al. An autoencoder based model for detecting fraudulent credit card transaction / Procedia Computer Science, 2020. Vol. 167, P. 254-262. URL: https://www.sciencedirect.com/science/article/pii/S1877050920306840/pdf?md5=72e32da2744bcbef307050473d4b8679&pid=1-s2.0-S1877050920306840-main.pdf

3 Fanai H., Abbasimehr H. A novel combined approach based on deep Autoencoder and deep classifiers for credit card fraud detection / Expert Systems with Applications. 2023. Vol. 217, P. 119562 URL: https://www.sciencedirect.com/science/article/pii/S0957417423000635

4 John H., Naaz S. Credit card fraud detection using local outlier factor and isolation forest / Int. J. Comput. Sci. Eng. 2019. Vol. 7, №. 4. P. 1060-1064. – Access mode: https://www.researchgate.net/profile/Sameena-Naaz-4/publication/335809102_Credit_Card_Fraud_Detection_using_Local_Outlier_Factor_and_Isolation_Forest/links/695e419ea1fd01798911addf/Credit-Card-Fraud-Detection-using-Local-Outlier-Factor-and-Isolation-Forest.pdf

5 Ounacer S. et al. Using Isolation Forest in anomaly detection: the case of credit card transactions / Periodicals of Engineering and Natural Sciences. 2018. Vol. 6, №. 2. URL: https://pen.ius.edu.ba/index.php/pen/article/download/1757/1236

6 Credit Card Fraud Detection URL: https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud

7 Link to the program code URL: https://github.com/IrinaGorpinich/Hybrid_Fraud_Detection/blob/main/main.py

8 Hossin M. A review on evaluation metrics for data classification evaluations / International journal of data mining & knowledge management process. 2015. Vol. 5, № 2. P. 1. URL: https://www.academia.edu/download/37219940/5215ijdkp01.pdf