Journal of Advances in Science and Technology
Vol.23, Issue No. 1 March-2026, ISSN 2230-9659

Leveraging Artificial Intelligence and Machine Learning for Real-Time Fraud Detection in E-Commerce Transactions

Sachin Bagoria[1]*, Dr. Kavita[2]

1 Research Scholar, SKD University, Hanumangarh, Rajasthan, India

radheykrishnalalita@gmail.com

2 Professor, SKD University, Hanumangarh, Rajasthan, India

Abstract: With more and more people making purchases online, fraud detection has become an important issue for online marketplaces due to the explosion of e-commerce. However, traditional approaches often are inadequate for catching more sophisticated and emerging fraudulent activities in real-time. The aim of this research is to investigate the effectiveness of ML and AI techniques in real-time detection of online shopping fraud. The number of 50,000 records were selected from marketplaces using stratified sampling to ensure representative sampling of classes. Data preparation involved dealing with missing data, removing duplicate data, address outliers, scaling features, and encoding categorical data for analysis. To overcome the problem of class imbalance, the use of SMOTENC, SMOTENC + ENN, & SMOTENC + Tomek Links approaches were performed. Numerous ML classifiers, such as Random Forest & Stochastic Gradient, were tested. The model was assessed for several parameters such as recall, accuracy, precision, F1 score, and AUC-ROC. Random Forest (RF) out performed all the other classifiers in both balanced and unbalanced datasets and Stochastic Gradient (SG) performed the next best. The most important factors that go into fraud detection judgements were determined via SHAP analysis. The study highlights potential opportunities for trust in e-commerce platforms, risk mitigations in terms of financial losses, and enhanced transaction security through AI-driven fraud detection.

Keywords: Artificial Intelligence, Machine Learning, Fraud Detection, E-Commerce Transactions, Random Forest, SMOTENC, SHAP Analysis, Class Imbalance, Cybersecurity, Predictive Analytics.

1. INTRODUCTION

In recent ten years, e-commerce has emerged as one of the fastest-growing segments in the global economy, growing from around 0.5% of GDP in the world to more than 1.5% [1]. There are advantages that companies and customers can offer to online shopping and digital payment systems & electronic transactions and those possibilities have been expanding rapidly in recent years. However, this growth has been accompanied by the emergence of cybercrime and fraudulent activities. Due to the increasing danger of online fraud, the projected worldwide cost of cybercrime jumped from $445 billion in 2014 to over $600 billion in 2017.

Examples of some of the many forms of malicious activity encompassed by the term 'e-commerce fraud' include: fraudulent listing creation, fraudulent reviews, account takeover attacks, fraudulent payments and fraudulent accounts [3, 4]. This has caused businesses to deal with massive monetary losses and online marketplaces lose credibility and consumer confidence. As the number of transactions has increased at an exponential rate, the traditional rule-based fraud detection systems which fail to detect complex and evolving fraud scenarios have also become inadequate.

The use of AI and ML in detecting, preventing and mitigating fraudulent activities on online marketplaces has increased by a huge margin. Fraud detection systems are widely adopted by large companies like Microsoft [5], LinkedIn [6] and eBay [7] that use machine learning to make their systems more efficient. These systems are able to quickly detect any fraudulent actions by analysing massive amounts of behavioural and transactional data, finding unusual patterns, and drawing conclusions.

Problems with fraud datasets' extreme imbalance and the ever-increasing complexity of fraud schemes persist despite substantial progress in the field of fraud detection. It is challenging for machine learning algorithms to correctly detect minority-class occurrences since fraudulent transactions usually only account for a tiny proportion of overall transactions. Therefore, using good data preparation, class balancing tactics, feature engineering, & model interpretability methodologies is crucial for developing strong fraud detection systems.

Within this framework, the current research delves into the use of AI and ML for the purpose of detecting online transaction fraud in real-time. It features a comprehensive experimental setup, data preparation, stratified sampling, stratified majority minority sampling (SMOTENC) techniques to handle class imbalance, and evaluation of multiple machine learning classifiers. In addition, the most important characteristics that go into fraud detection judgements are identified using SHAP analysis. The aim of this study is to propose a classification algorithm and rebalancing procedures comparison that can be useful in the design of a practical and understandable solution to improve the performance of e-commerce fraud detection.

This study's findings are expected to contribute to the creation of a reliable AI-powered fraud detection system, which will help enable safe online transactions, minimise financial losses and boost consumer confidence in online shopping platforms.

2. OBJECTIVES

- To create and assess machine learning and artificial intelligence models for real-time fraud detection in online transactions.
- To evaluate how well various class-balancing strategies & machine learning classifiers enhance fraud detection efficiency and model interpretability.

3. RESEARCH METHODOLOGY

In order to create and assess ML and AI models for e-commerce fraud detection in real-time, this study uses a quantitative & experimental research approach. Examining numerical and categorical transaction variables and evaluating the performance of different machine learning algorithms in various data-balancing procedures is the main emphasis of the study, which aims to uncover fraudulent actions [8].

3.1 Data Collection

Listing information and transaction data from an online marketplace are included in the data collection. For fair and efficient distribution the selected sample of 50,000 records were randomly selected from the overall data set using a stratified sampling technique. Using stratified sampling, we were able to guarantee that our sample was representative of all types of transactions and fraud.

3.2 Data Preprocessing

A comprehensive pretreatment pipeline was developed to prepare the data for the analysis under machine learning. Some of the preprocessing techniques employed include:

- Elimination of duplicates.
- What does happen when the data is missing?
- Identification and control of outliers.
- Categorical variables are converted to numbers.
- Normalisation and scaling of continuous variables.

- User behaviour pattern based feature extraction and selection based on transaction attributes.

The same pre-processing procedure was applied throughout all the stages of the experiment.

3.3 Handling Class Imbalance

To address the issue of class imbalance, data-level rebalancing techniques were employed, as the transactions that are fraudulent are a minority class. There were three ways of oversampling:

- Synthetic Minority Oversampling Technique for Nominal & Continuous Features or SMOTENC.
- Nearest Neighbours (NN) + SMOTE (Nearest Neighbours with noise) + Edited Nearest Neighbours (ENN).
- Tomek + SMOTENC Links.

These techniques were used to adjust the ratio between the number of fraudulent and non-fraudulent transactions, which improved model learning and reduced categorisation bias.

3.4 Model Development

To identify fraud, a number of machine learning classifiers were created and assessed. The performance of several classification algorithms was compared in the study, including:

- The Random Forest Classifier.
- Classifier using Stochastic Gradient (SG).
- Additional benchmark models for categorization.

To evaluate the effect of class balancing upon fraud detection performance, each classifier underwent training using both the original & rebalanced datasets.

3.5 Experimental Setup

There were four phases to the experiments:

Experiment 1: Classifiers are trained and evaluated on the original data preprocessed.

Experiment 2: Applying the processed data for feature engineering & model optimisation.

Experiment 3: Class Imbalance correction techniques using SMOTENC and retraining classifiers.

Experiment 4: Evaluation of hybrid resampling techniques (SMOTENC + ENN & SMOTENC + Tomek Links), followed by a comparison of the performances of the classifiers.

3.6 Model Evaluation Metrics

The models were evaluated by the both in-sample & out-of-sample datasets. The following standards of categorisation were used to assess a performer's performance:

- Precision.
- Accuracy.
- Remember.
- The F1-Score.
- AUC-ROC (Area Under Receiver Operating Characteristic Curve).

Thanks to the comparison study, the best approach to classification and balancing for fraud detection was identified.

3.7 Feature Importance Analysis

The model was improved to be more interpretable by using feature significance analysis [9]. The top 10 factors that were most important for fraud detection were identified using Feature significance scores & SHAP (SHapley Additive Explanations) values.

The explanation of model predictions was done by applying SHAP analysis, with the following conditions:

- A positive SHAP value was more likely to be considered fraudulent.
- Negative SHAP values were more likely to be considered not fraudulent.

3.8 Data Visualization and Trend Analysis

Analyzed the trends and pattern of fraud and transactions using visualisation tools. Monthly demand heatmap were created to facilitate the comparison of transactions on weekdays and across seasons. These were useful for identifying when the transactions were high, and for understanding consumers' purchase patterns.

3.9 Statistical and Comparative Analysis

In order to compare efficiency of each resampling method and each classifier, comprehensive analysis was made. Results indicated that the performance of fraud detection using the Random Forest classifier is better than using the Stochastic Gradient classifier for both the balanced and unbalanced datasets. The robustness and generalisability of the model were checked using comparative analysis utilising in-sample and out-of-sample assessment outcomes.

3.10 Ethical Considerations

The data in all transactions were anonymised before analysis. All information was anonymous and research was conducted in an ethical manner.

4. RESULT

In order to ensure that all subgroups are adequately represented, we use stratified sampling to choose 50,000 rows at random from the Marketplace listing data. This is done for the purpose of the fast-computing experiment. Within the scope of this study, our primary focus is on developing a model for the identification of fraudulent activity by using numerical & categorical characteristics [10–12]. Our first step will be to search the listings data for these traits and compare them to the demographics, behaviours, and purchases made by marketplace users. A distinct pipeline is responsible for the processing of trials 1 and 2, the encoding of categorical variables, the scaling of continuous features, the handling of outliers, duplicates, & missing data, & so on.

In order to fix class asymmetry, the third and fourth experiments use an extra pipeline that uses oversampling and/or undersampling to equalise the minority and majority class ratios. Despite the fact that SMOTENC, SMOTENC + ENN, and SMOTENC + TomekLinks all get a score of 90% when working with in-sample data, they all fall short when coping with out-of-sample

data, achieving only approximately 55%. The Random Forest algorithm surpasses every other classifier-rebalancing system when applied to both in-sample and out-of-sample data, as well as every performance evaluation evaluation. When compared to other classifiers, the SG classifier comes in second position overall [13]. None of the competing classifiers demonstrate any discernible improvement across all comparison points. We provide comprehensive performance data in Fig. 1, which is located below.

Table 1: Comparative Performance of Classifiers under Different Rebalancing Techniques

Classifier	**RandomOverSampler**	**SMOTENC**	**SMOTENC + ENN**	**SMOTENC + TomekLinks**
LR	Moderate	Moderate	Moderate	Moderate
KNN	Good	Good	Very Good	Very Good
CART	Low	Low	Low	Low
RF	Good	Good	Good	Good
SVC	Excellent	Excellent	Excellent	Excellent
GNB	Low	Low	Low	Low
GBC	Excellent	Excellent	Excellent	Excellent
SG	Moderate	Moderate	Moderate	Moderate

Table 1 shows the performance of various machine learning classifiers, under different class rebalancing strategies. Among all the balancing strategies, the Support Vector Classifier (SVC) & Gradient Boosting Classifier (GBC) were the best. Also, Random Forest (RF) was found to be consistent and reliable and rose to become a prominent classifer in fraud detection. The Hybrid Balancing techniques such as ENN and Tomek Links along with SMOTENC have resulted in better performance for K-Nearest Neighbours (KNN). GNB and CART, on the other hand, had also a much lower performance than all the rebalancing schemes. According to these results, when it comes to identifying fraudulent transactions in skewed e-commerce datasets, ensemble-based and sophisticated classification algorithms work better.

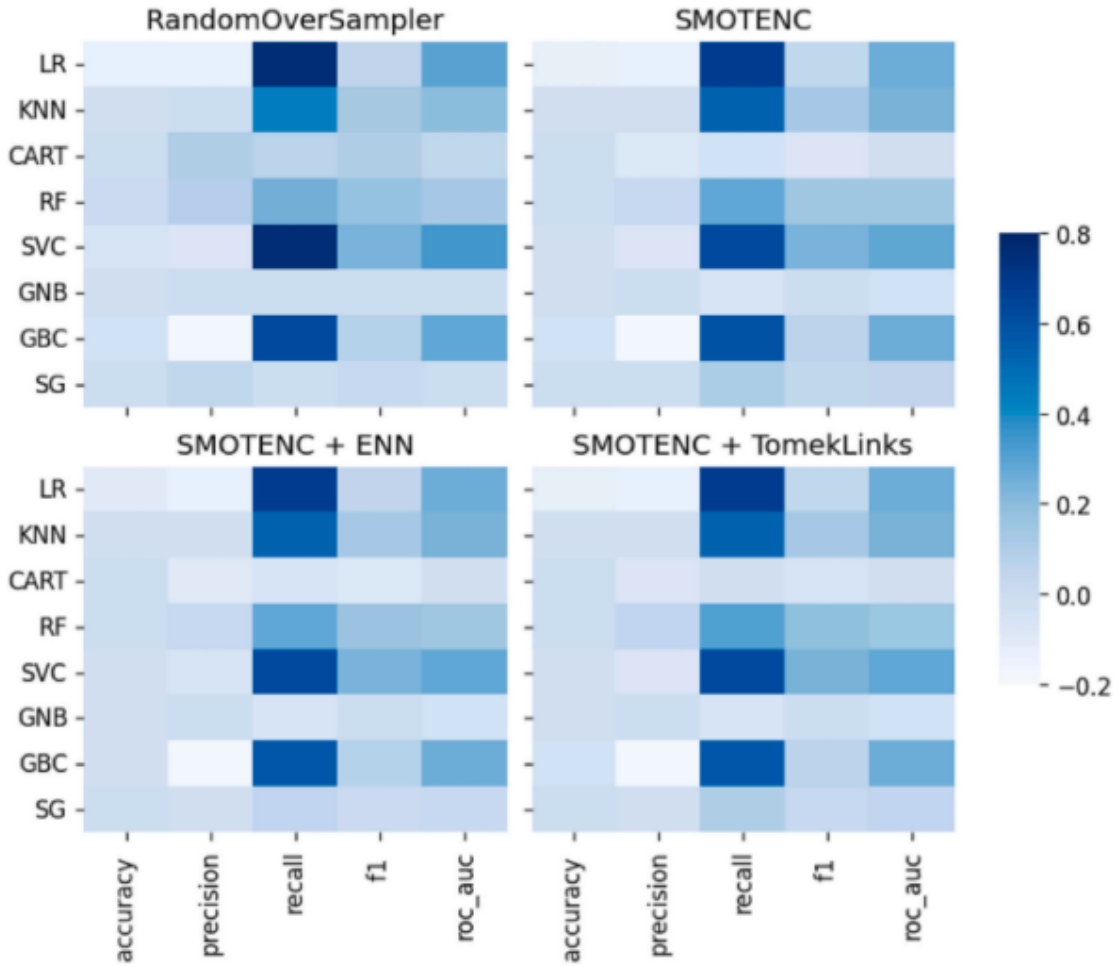

Figure 1: Each classifier's improvement in out-of-sample performance for a particular data-level class rebalancing approach.

Figure 2 shows a monthly demand heatmap that displays the demand for weekdays. This particular online shop had a perceptible increase in demand from the month of December to the month of May. It is typical for things to get quite chaotic in the beginning of April [14]. When businesses are in possession of all the relevant information, they are also in a position to take the right actions to encourage customers to make purchases at various times.

Table 2: Monthly Transaction Demand by Weekday

Weekday	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Sunday	339	268	566	619	559	194	231	189	100	328	165	215
Monday	252	244	540	660	564	191	163	183	118	250	159	231
Tuesday	280	314	651	611	390	189	192	133	150	219	156	190
Wednesday	218	285	555	569	430	200	195	144	127	252	123	207
Thursday	262	262	534	696	314	225	208	141	139	187	163	222
Friday	277	241	530	693	319	215	313	123	120	255	168	243
Saturday	286	250	514	797	406	176	325	144	129	243	144	181

Monthly and weekly trends in transaction demand are seen in Table 2. The results showed that the volume of transactions has risen considerably from January to April, with April having the highest overall demand. The busiest day of the month of April was definitely when customers were the busiest with 797 transactions. Beginning in May, demand dropped steadily until it hit rock bottom in August and September. The study indicates that the heat map also shows some degree of seasonal buying behaviour and that there is some months when there are increased transactions. In order to maximise inventory management, promotional marketing, & fraud monitoring efforts throughout peak transaction times, e-commerce enterprises might benefit from understanding these demand swings.

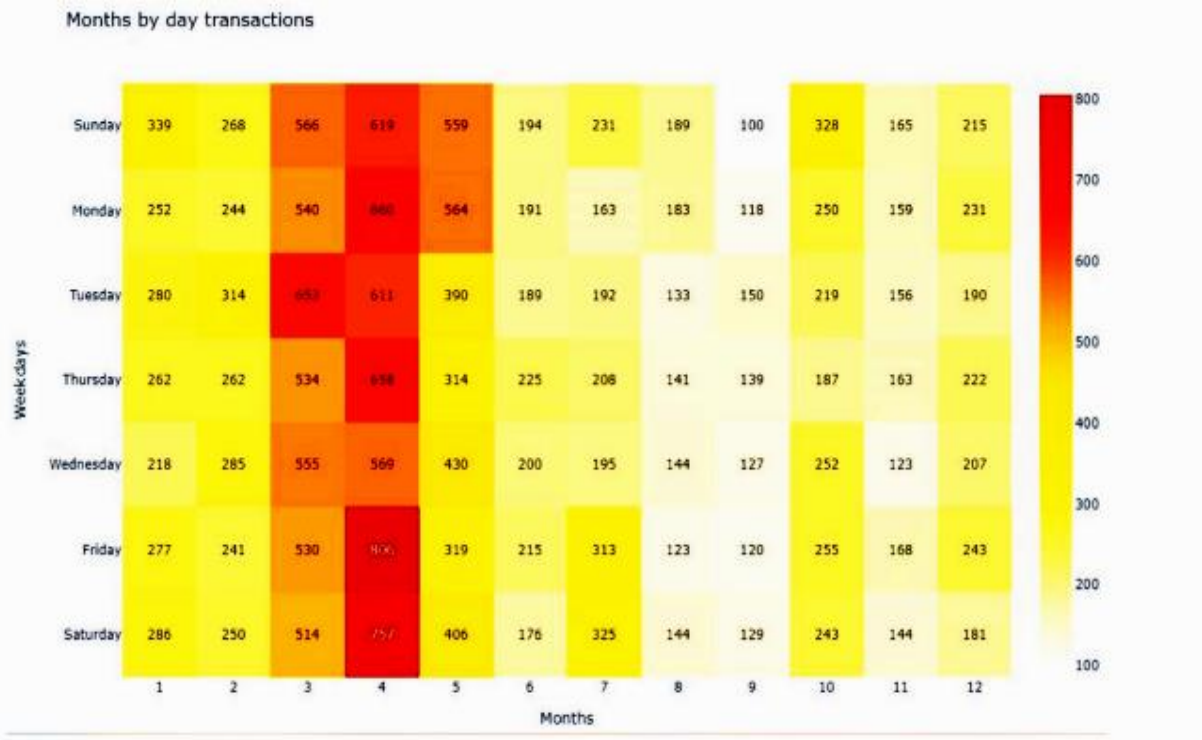

Figure 2: Transaction heatmap for a single online business.

The top 10 traits are responsible for our model's remarkable performance in recognising instances of fraudulent activity, as seen in the global feature significance plot that can be found in Figure 3.

Table 3: Top Features Influencing Fraud Detection

Rank	Feature	Mean SHAP Value
1	median_bsg_size	1.28
2	mp_tab_initial_messages_30d	0.78
3	account_age	0.75
4	friend_count	0.41
5	initial_price	0.39
6	good_seller_rating_received_lifetime	0.34
7	largest_bsg_size	0.28
8	seller_selected_condition [new]	0.27
9	age	0.16

10	Sum of 23 Other Features	0.14

Based on SHAP values, Table 3 shows the most significant factors that contribute to fraud detection. The feature median_bsg_size had a significant impact on the model's fraud prediction capacity, as shown by its high relevance score of 1.28. Other significant predictors were initial price (0.39), friend count (0.41), account age (0.75) and mp_tab_initial_messages_30d (0.78). These variables are based on user actions, account information and transaction characteristics that are closely associated with fraud. The SHAP analysis not only enhances the interpretability and reliability of the fraud detection framework, but it also contributes to the transparency of the model.

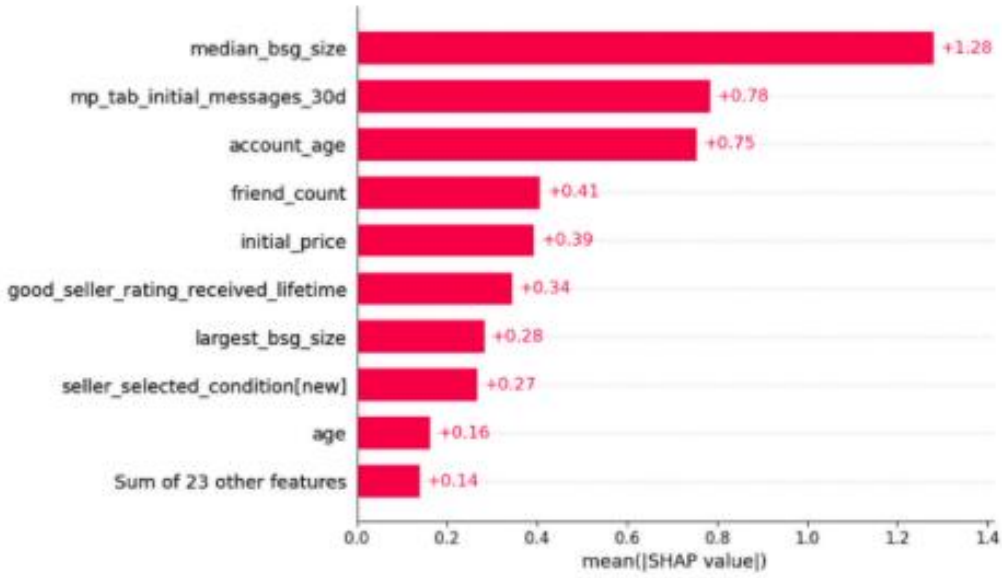

Figure 3: Crucial elements affecting the identification of fraudulent cases

In the event that the SHAP value is negative, the chance of the model predicting a non-fraudulent instance is raised. On the other hand, the likelihood of the model predicting a fraudulent instance is enhanced when the SHAP value is positive [17].

5. CONCLUSION

The use of machine learning and artificial intelligence (AI) was demonstrated in this study as effective tools in real-time detection of online shopping fraud. Using multiple classification algorithms, class imbalance handling methods and comprehensive data pre-processing

techniques, the study determined that Random Forest was the most effective model for detecting fraudulent activity. SHAP analysis helped to understand the models better by highlighting the most important characteristics related to fraud, while rebalancing strategies based on SMOTENC boosted the performance of the model during the study and classification. The results show that online marketplaces may considerably improve their transaction security, reduce financial losses, and help with trustworthy decision-making with the use of fraud detection systems powered by artificial intelligence. To counteract these more complex kinds of fraud, e-commerce systems may benefit from using powerful machine learning algorithms.

References

1. Moagar-Poladian, S., Dumitrescu, G. C., & Tanase, I. A. (2017). Retail e-commerce (e-tail): Evolution, characteristics and perspectives in China, the USA and Europe. *Global Economic Observer*, *5*(1), 167–178.

2. McAfee. (2018). *The economic impact of cybercrime—No slowing down*. https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf

3. Cavico, F. J., & Mujtaba, B. G. (2017). Wells Fargo's fake accounts scandal and its legal and ethical implications for management. *SAM Advanced Management Journal*, *82*(2), 4–14.

4. Kawase, R., Diana, F., Czeladka, M., Schüler, M., & Faust, M. (2019). Internet fraud: The case of account takeover in online marketplace. In *Proceedings of the 30th ACM Conference on Hypertext and Social Media* (pp. 181–190).

5. Nanduri, J., Jia, Y., Oka, A., Beaver, J., & Liu, Y. W. (2020). Microsoft uses machine learning and optimization to reduce e-commerce fraud. *INFORMS Journal on Applied Analytics*, *50*(1), 64–79.

6. Wang, R., Nie, K., Wang, T., Yang, Y., & Long, B. (2020). Deep learning for anomaly detection. In *Proceedings of the 13th International Conference on Web Search and Data Mining* (pp. 894–896).

7. Porwal, U., & Mukund, S. (2019). Credit card fraud detection in e-commerce. In *2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)* (pp. 280–287). IEEE.

8. Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: A review of anomaly detection techniques and recent advances. *Expert Systems with Applications, 193*, 116429.

9. Ashtiani, M. N., & Raahemi, B. (2022). Intelligent fraud detection in financial statements using machine learning and data mining: A systematic literature review. *IEEE Access, 10*, 72504–72525.

10. Albashrawi, M. (2016). Detecting financial fraud using data mining techniques: A decade review from 2004 to 2015. *Journal of Data Science, 14*(3), 553–570.

11. Choi, D., & Lee, K. (2018). An artificial intelligence approach to financial fraud detection under IoT environment: A survey and implementation. *Security and Communication Networks, 2018*, 1–15.

12. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems, 50*(3), 559–569.

13. Ryman-Tubb, N. F., Krause, P., & Garn, W. (2018). How artificial intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark. *Engineering Applications of Artificial Intelligence, 76*, 130–157.

14. Al-Hashedi, K. G., & Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. *Computer Science Review, 40*, 100402.

15. Chaquet-Ulldemolins, J., Moral-Rubio, S., & Muñoz-Romero, S. (2022). On the black-box challenge for fraud detection using machine learning (II): Nonlinear analysis through interpretable autoencoders. *Applied Sciences, 12*(8), 3856.

16. Da'u, A., & Salim, N. (2020). Recommendation system based on deep learning methods: A systematic review and new directions. *Artificial Intelligence Review*, *53*(4), 2709–2748.

17. Zeng, Y., & Tang, J. (Year). RLC-GNN: An improved deep architecture for spatial-based graph neural network with application to fraud detection.