**Journal of Economic Theory and Business Management**
**ISSN 3006-4953 (Print) | ISSN 3006-4961 (Online) | Vol. 1, No. 2, 2024**

SUAS Press

# Fraud Detection in Digital Payment Technologies Using Machine Learning

**WANG, Junliang** [1*]

[1] Johns Hopkins University, USA

***** WANG, Junliang is the corresponding author, E-mail: jwang386@alumni.jh.edu***

**Abstract:** Data has become the banking industry's most valuable asset, not only helping banks attract more customers, increase the loyalty of existing customers, make more effective data-driven decisions, but also enhancing business capabilities, increasing operational efficiency, improving existing services, enhancing security, and generating more revenue through all of these actions, and more. This paper explores the application of machine learning and artificial intelligence techniques in fraud detection in the financial sector. By analyzing the characteristics and common scenarios of financial fraud, the accuracy and efficiency of fraud detection model are improved by using dynamic integrated selection and double error measurement. The experimental results show that the machine learning model performs well in financial fraud detection, providing financial institutions with a more reliable and secure transaction environment, protecting the interests of customers and the stability of the financial market.

**Keywords:** Financial fraud, Machine learning, Dynamic integration selection, Double error measure

**DOI:** https://doi.org/10.5281/zenodo.10926495

# 1 INTRODUCTION

Accounting fraud is a worldwide problem. If not detected and prevented in time, it will not only cause significant damage to the stakeholders of fraudulent enterprises, but also indirectly cause significant damage to the stakeholders of many non-fraudulent enterprises. With the rapid development of the Internet and mobile Internet, the digital process of business activities has also been developed rapidly, and e-commerce has now become an important part of daily economic activities. [1]With that, however, comes cybercrime, which reportedly costs the global economy $600 billion a year, or about 0.8% of global GDP, with fraud against banks and consumers costing billions of dollars a year, not including indirect losses, as well as the digital brand risk for banks that lose the trust of their customers.

It is worth noting that the above fraud is often achieved through social engineering such as fake official websites, apps, and key employees, rather than high-tech intrusion. [2,3] Detecting fraud in the dynamic and massive online economic activity has become an important challenge for the financial industry. However, the difficulty is not impossible to achieve, let's take a look at how the application of machine learning and artificial intelligence is a good practice for detecting fraud in the financial sector.

Through this research, we explore how machine learning and artificial intelligence techniques can be used to address the fraud challenges facing the financial sector. [4-6] Machine learning and artificial intelligence have become key tools for detecting fraud in financial transactions, enabling rapid and accurate identification of potential frauds in large-scale, dynamic online economic activity. Through the study of data sets and the analysis of specific patterns, we are able to effectively monitor and predict possible fraud in financial transactions, thereby providing financial institutions with a more reliable and secure trading environment, protecting the interests of customers and maintaining the stability and credibility of the financial market. The purpose of this paper is to emphasize the important role of machine learning and artificial intelligence in the financial field, and to provide useful enlightenment for further research and practice in the future.

# 2 RELATED WORK

## 2.1 Current situation of financial fraud

"Fraudulent" behavior is contrary to the natural law of "honesty and trustworthiness." The legal regulation of this type of risk behavior has existed since ancient times. [7] For example, the Roman Law on "fraud" is related to the interpretation: "All tricks or deception for the purpose of causing the person concerned to be deceived or to commit errors in order to benefit themselves, is fraud." Article 193 of China's Criminal Law clearly stipulates that credit fraud refers to defrauding financial institutions of financing through the following ways for the purpose of illegal possession: fabricating false reasons for introducing funds, projects, etc.; The use of false economic contracts; Use of false supporting documents; Using a false property right certificate as a guarantee or repeating a guarantee that exceeds the value of the mortgaged property; Using loans for illegal and criminal activities; Impersonating others to apply for loans, etc. Generally speaking, credit fraud means that fraudsters falsify the background of credit demand through false carriers such as fake enterprises, fake projects and fake transactions. Or by providing false statements, false guarantees, false assessments to influence credit decisions and other ways to defraud, apply or misappropriate the credit of financial institutions.

From the perspective of credit, credit fraud of commercial banks includes external fraud and internal fraud. Commercial banks should prevent fraudulent acts of credit granting customers, prospective credit granting customers and other third parties externally, and prevent fraudulent acts of bank employees internally. [8-11]Credit fraud can be manifested by external fraud and internal fraud alone, or it can be manifested by internal and external fraud for the same event or series of events. In credit practice, the common manifestations of credit fraud include the following: credit fraud with false reasons such as fabricating funds and projects; Credit fraud using false economic contracts; Credit fraud using false documentation; The use of false property rights as security or repeated mortgage credit fraud. In terms of risk sources, credit fraud risk mainly includes internal and external factors, and finally manifests itself in two forms: internal fraud and external fraud. At present, under the new normal of economy, the credit fraud of commercial banks shows a trend of integration and cross-infection of internal and external fraud.

## 2.2 Fraud detection feature

In the financial sector, common scenarios for machine learning to prevent fraud include identifying fake websites, identifying fake apps, identifying fake social media accounts, identifying business email fraud, and identifying financial fraud.

Fake websites: Attackers use fake phishing websites to lure users to provide sensitive information such as name, phone number, ID number, online banking account, user name, password, etc., resulting in damage to corporate brands and user interests. [12,13] The arrival of the mobile era has also prompted the evolution of phishing techniques, the most obvious is the emergence of a large number of phishing websites adapted to the mobile phone interface, both in content and form are very similar to regular websites, users are often unable to distinguish.

Taking the UK's National Cyber Security Centre (NCSC) public data on the disposal of counterfeit websites in 2021 as an example, the top three counterfeit website attacks are: The National Lottery, the UK Financial Conduct Authority, and the Bank of England. It is important to note that this data represents the number of phishing activities detected and successfully handled by monitoring, not the total number of potentially viable phishing websites.

**Table 1.Summary of Cyberattacks on UK Government Entities and Related Organizations**

| Government Entity | Number of Attacks (URLs) |
|---|---|
| Government Brand | 511 |
| National Lottery | 459 |
| Financial Conduct Authority | 392 |
| Bank of England | 370 |
| Ministry of Justice | 123 |
| British Broadcasting Corporation | 4 |
| Metropolitan Police | 25 |
| Department for Exiting the European Union (Brexit) | 18 |
| HM Treasury | 37 |
| National Crime Agency | 25 |
| Prudential Regulation Authority | 18 |

1) Fake APP: Attackers develop fake enterprise apps, abuse brand logos and trademarks, distribute and download them through unauthorized channels, and try to defraud various victim users' bank card accounts, identity accounts, passwords and other private information.

2) Fake social media accounts: Attackers create fake corporate accounts on social media, or fake corporate executives, stars or celebrities, trying to defraud various victim users of bank card accounts, identity accounts, passwords and other private information.

3) Commercial email fraud: [14-16] Fraudsters use social engineering techniques to carry out phishing and fraud activities by registering domain names close to customer subjects and sending relevant emails. Unlike pure Email Spoofing (Email Spoofing, forging email headers, spreading phishing links or malicious attachments), this type of email spoofing tends to be more subtle, targeting people in key departments such as company management or finance.

4) Business fraud: Analyze large amounts of transaction data to find fraud patterns for real-time fraud detection. When the AI model suspects that a transaction is fraudulent, it can choose to reject the transaction or flag the transaction as suspicious for further investigation, and give potential reasons for assessing fraud, focusing limited investigator work time on the instances that are most likely to be fraudulent; [17]AI models provide cause codes for flagged suspicious transactions that can guide investigators to speed up investigations; Ai can also learn and revise its knowledge models as investigators evaluate and remove suspicious transactions, improving the accuracy of identifying fraud.

## 2.3 Fraud detection using machine learning

"Artificial intelligence will be the ultimate version of Google. The ultimate search engine that understands everything on the web. It will understand exactly what you want, and it will give you the right thing. We are far from that now. But we can gradually get closer to that point, and that's basically our job." -- Larry Page, co-founder and developer of Google.

Because ML algorithms are able to learn from historical fraud patterns and identify them in future transactions, fraud detection using machine learning becomes possible. In terms of information processing speed, machine learning algorithms appear to be more efficient than humans. In addition, machine learning algorithms are able to detect complex fraud features that humans simply cannot detect.

Work faster. A rules-based fraud prevention system means creating precise written rules that "tell" the algorithm which types of operations look normal and should be allowed, and which shouldn't because they look suspicious. However, writing rules takes a lot of time. Moreover, manual interactions in the e-commerce world are so dynamic that things can change significantly in a matter of days. Here, machine learning fraud detection methods will come in handy to learn new patterns.

Scale. ML methods show better performance as the data sets they fit grow - meaning that the more samples of fraudulent operations they accept, the better their ability to identify fraud. The principle does not apply to rules-based systems, as long as they never evolve on their own. In addition, data science teams should be aware of the risks associated with rapid model scaling; If the model does not detect fraud and incorrectly flags it, this will lead to underreporting in the future.

Efficiency. Machines can take over the repetitive work of routine tasks and human fraud analysis, and experts will be able to spend their time making more advanced decisions [18].

The aim of this study was to identify the most effective models for identifying corporate fraud in China. We combine raw and non-financial data and use a variety of basic classifiers to evaluate and compare. Our focus is on evaluating the performance of the dynamic integration model, which performs best across four typical evaluation metrics. We call it the DES model, which has demonstrated excellent performance in fraud detection. Our findings help regulators more effectively identify and detect companies engaging in fraudulent activity.

# 3 METHODOLOGY

3.1 Dynamic integration selection

Here, we employ the algorithm utilized in generative artificial intelligence financial robots for fraud detection. The applicability of this algorithm has been validated through experiments in related fields [19]. DES classifiers are superior to individual logistic regression or static ensemble classifiers in many ways, including the ability to capture local areas, take advantage of the diversity and complementarity of basic classifiers, reduce overfitting, dynamically adapt to data changes, and efficiently process noisy data.

The steps of DES algorithm can be divided into three points, as shown in Figure 1. First, you need to select a basic set of classifiers trained on a subset of the available data. Second, in the classification phase, the DES algorithm selects a subset of the basic classifier for the instance to be classified based on the past performance of each instance on similar instances. Finally, the algorithm combines the output of the specified basic classifier to obtain the final classification output. Overall, the key idea behind DES is to use the most accurate classifier for each instance, while avoiding classifiers that might make mistakes on that particular instance. This also means that DES can adapt to the changing data distribution and obtain better resolution accuracy than a single classifier [20].

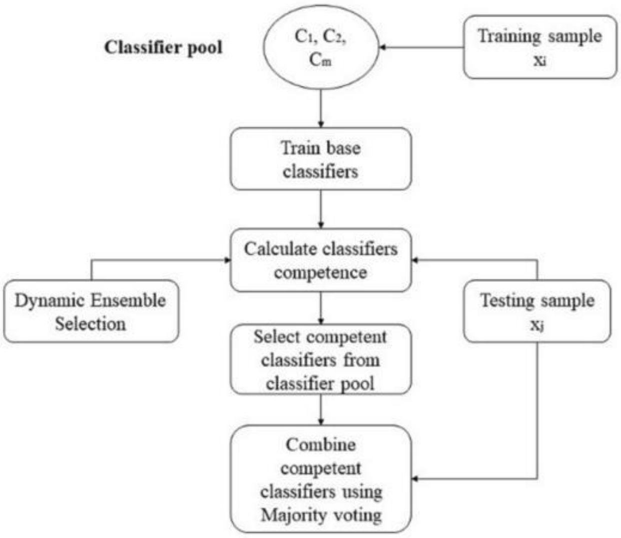
Classifier pool
C1, C2, Cm
Training sample xi
Train base classifiers
Calculate classifiers competence
Dynamic Ensemble Selection
Testing sample xj
Select competent classifiers from classifier pool
Combine competent classifiers using Majority voting

**Figure 1: DES classifier architecture diagram**

## 3.2 DF metric

A DF measure, also known as a "double error" measure, is a situation in which two or more basic classifiers in an integrated model make incorrect predictions about the same instance. In the fraud detection literature, we have identified eight different basic classifiers, including logistic regression, balanced bagging, XGBoost, Ridge classifiers, RusBoost, random forests, GBRT, and support vector machines. However, one of the goals of this paper is to identify the basic classifiers that make up the dynamic integration model (DES). Therefore, we introduce DF metrics to evaluate the performance of these basic classifiers. Our attempt on this method was inspired by Zengyi Huang et al., where the modification of the K-cluster algorithm for DF metrics played a significant role [21]. The lower the value of the DF measure, the classifiers are more accurate at predicting the correct category, that is, they produce fewer "double errors" and have greater predictive power than other classifiers in the ensemble.

### 3.3 Data Preprocessing

**Table 2. Fraud distributions.**

| Year | No. of listed firms | No. of fraud offenders | Percentage of fraud |
|---|---|---|---|
| 2007 | 747 | 36 | 4.28% |
| 2008 | 867 | 34 | 4.61% |
| 2009 | 960 | 55 | 3.75% |
| 2010 | 1059 | 80 | 3.21% |
| 2011 | 1424 | 228 | 3.87% |
| 2012 | 1722 | 350 | 4.65% |
| 2013 | 1795 | 418 | 6.07% |
| 2014 | 1707 | 374 | 7.50% |
| 2015 | 1814 | 250 | 12.57% |
| 2016 | 1896 | 245 | 16.82% |
| 2017 | 1998 | 253 | 17.52% |
| 2018 | 2213 | 394 | 18.89% |
| 2019 | 2218 | 294 | 16.86% |
| 2020 | 1909 | 587 | 13.10% |

According to the data in the above table, the fraud, raw financial and non-financial data in this article are derived from CSMAR, but do not include the MD&A tone from CNRDS (China Research Data Service Platform) and the internal control index from DIB database. In the definition of fraud, we assign a value of 1 to regulators sanctioning the company for fraud in a given year, and 0 to regulators otherwise. After further observing the fraud sample, it is not difficult to find, as shown in Table 1, that the number of frauds has increased sharply since 2015. This paper also provides two explanations for this. First, the [22] IPO market improved the overall health of the market before reopening in January 2014; Second, in October 2013, the China Securities Regulatory Commission granted more than 30 agencies the power to sanction fraudulent companies, leading to an increase in fraud identification.

In addition, during the study period, the fraud sample accounted for about 11%, which is significantly higher than 1% in the United States, because CSMAR includes all types of fraud, but AAER only discloses serious and significant fraud. In order to make our data comparable to that of the United States, we also focused on continuous crime, which is defined as more than one fraud in a year and assigned a value of 1 and 0 if not. In this case, the serial offender fraud sample was reduced to 587 companies, or about 2.9 percent of the company years.

## 3.4 Model training

The training period of this paper is from 2007 to 2015, the validation period is from 2016 to 2017, and the testing period is from 2018 to 2020. We use the training period to train the models, and the validation period to determine the best parameters for each model. After obtaining the best parameters for each model, we tested it during out-of-sample testing from 2018 to 2020. Figure 2 Training framework diagram below.

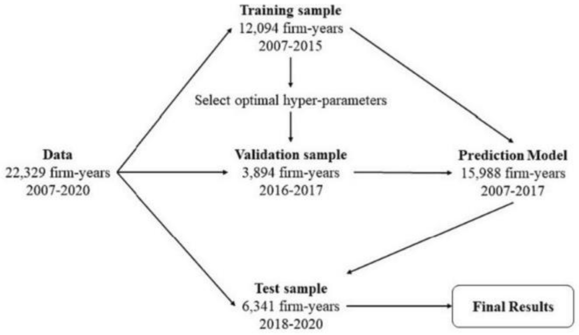

Figure 2. Training model architecture diagram

First, the ROC curve. The ROC curve and true positive rate are plotted by using various classification thresholds. The closer the curve is to the top left corner of the chart, the better the performance of the model. The ROC curve can also be reduced to a single value: AUC (i.e. area under the ROC curve). The principle is that randomly selected fraudulent companies have a higher probability of predicting fraud than randomly selected non-fraudulent companies. AUC scores range from 0 to 1, with a random guess of 0.5, but in order for the model's results to be meaningful, they should score higher than 0.5. Second, PR curve. The closer the PR curve is to the top right corner of the chart, the better the model. Similarly, the PR curve can be reduced to a single value: AP. AP scores range from 0 to 1, with higher scores indicating better performance. Unlike AUC, AP is sensitive to changes in class distribution and data set balance, and it is more appropriate when few class frauds are rare. Third, MCC index. This indicator is an effective way to evaluate the relationship between the actual value and the predicted value.

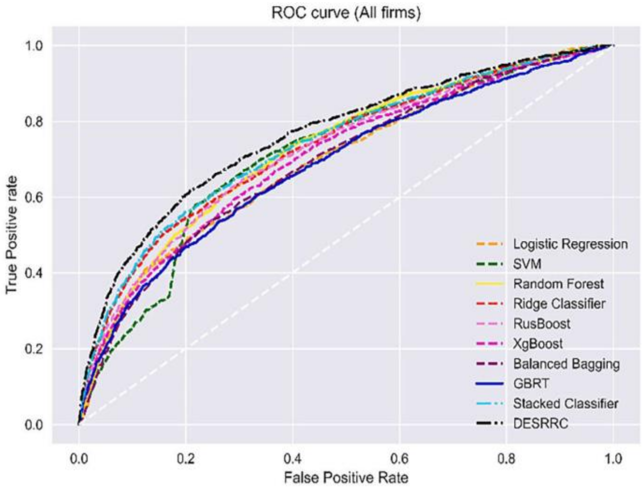

**Figure 3.ROC curve results**

Results show the top 16.4% of results. Six percent of the results showed that DESRRC and stack classifiers were the best-performing models, with scores of 0.485 and 0.441, respectively, indicating that the DES model was more effective at ranking fraudulent companies in the top 16. In addition, under the Precision@k metric, we find that GBRT performs best (0.498), followed by DESRRC (0.475), also meaning that actual fraudulent companies can be accurately detected when the model ranks it in the top 16. At Recall@k, DESRRC remains the best model for correctly identifying the highest number of actual fraudulent companies (0.438), followed by RusBoost (0.396). In addition, as a robustness test, we further modified and reported performance metrics for the top 11% of companies, all with similar results. In general, DES model shows good performance under various performance evaluation indicators, that is, DES model may be very suitable for regulators, because it can effectively identify and detect companies engaged in fraudulent activities.

# 4 CONCLUSION

First, this paper explores in depth the fraud problems faced by the financial sector, especially with the rapid development of the Internet and mobile Internet, financial fraud has become a global challenge. However, through the application of machine learning and artificial intelligence technologies, we can effectively address this challenge. The study found that machine learning algorithms are able to learn fraud patterns from historical data and quickly and accurately identify potential fraud in large-scale, dynamic online economic activity. This provides financial institutions with a more reliable and secure trading environment, protects the interests of customers, and maintains the stability and credibility of the financial market.

Secondly, this paper introduces key techniques such as dynamic integrated selection and double error measurement, through which we are able to improve the accuracy and adaptability of fraud detection models. The experimental results show that the dynamic integration model performs well in ranking fraudulent companies with high accuracy and reliability. Therefore, we believe that machine learning and artificial intelligence technologies will play an increasingly important role in the financial sector, bringing more innovation and progress to the financial industry.

In the future, with the continuous progress of technology and the continuous accumulation of data, the application of machine learning and artificial intelligence technology in the financial field will show more possibilities and potential. First, we can further optimize and improve the fraud detection model to improve its recognition ability and adaptability to new fraud behaviors. Second, we can explore more data sources and feature engineering methods to further improve the performance and effectiveness of the model. In addition, with the development of blockchain technology, we can also combine it with machine learning technology to build a more secure and reliable financial transaction system and further reduce the risk of fraud. At the same time, we can also strengthen the interpretability and explainability of machine learning models to improve their credibility and reliability in financial decision-making and risk management.

# Acknowledgments

I would like to express my sincere thanks to Huang, Che and their co-authors for their research in the field of artificial intelligence for financial fraud detection. Their algorithms and experimental results have greatly assisted our research[19].

# Funding

Not applicable.

# Institutional Review Board Statement

Not applicable.

# Informed Consent Statement

Not applicable.

# Data Availability Statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

# Conflict of Interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

# Publisher's Note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

# Author Contributions

Not applicable.

# About the Authors

**WANG, Junliang**

International Economics & International Political Economy, Johns Hopkins University, DC, USA.

# References

[1] Yu, Liqiang, et al. "Stochastic Analysis of Touch-Tone Frequency Recognition in Two-Way Radio Systems for Dialed Telephone Number Identification." arXiv preprint arXiv:2403.15418 (2024).

[2] Xu, Xiaonan, et al. "AI Empowered of Advancements in Microbial and Tumor Cell Image Labeling for Enhanced Medical Insights." Journal of Theory and Practice of Engineering Science 4.03 (2024): 21-27.

[3] Che, Chang, et al. "Enhancing Multimodal Understanding with CLIP-Based Image-to-Text Transformation." Proceedings of the 2023 6th International Conference on Big Data Technologies. 2023.

[4] Xu, Xiaonan, et al. "Comprehensive Implementation of TextCNN for Enhanced Collaboration between Natural Language Processing and System Recommendation." arXiv preprint arXiv:2403.09718 (2024).

[5] Zeng, Q., Sun, W., Xu, J., Wan, W., & Pan, L. (2024). Machine Learning-Based Medical Imaging Detection and Diagnostic Assistance. International Journal of Computer Science and Information Technology, 2(1), 36-44.

[6] Che, Chang, et al. "Deep learning for precise robot position prediction in logistics." Journal of Theory and Practice of Engineering Science 3.10 (2023): 36-41.

[7] Wu, Jiang, et al. "Case Study of Next-Generation Artificial Intelligence in Medical Image Diagnosis Based on Cloud Computing." Journal of Theory and Practice of Engineering Science 4.02 (2024): 66-73.

[8] Shen, Xinyu, et al. "Biology-based AI Predicts T-cell Receptor Antigen Binding Specificity." Academic Journal of Science and Technology 10.1 (2024): 23-27.

[9] Su, G., Wang, J., Xu, X., Wang, Y., & Wang, C. (2024). The Utilization of Homomorphic Encryption Technology Grounded on Artificial Intelligence for Privacy Preservation. International Journal of Computer Science and Information Technology, 2(1), 52-58.

[10] Che, Chang, et al. "Advancing Cancer Document Classification with R andom Forest." Academic Journal of Science and Technology 8.1 (2023): 278-280.

[11] Cheng, Q., Gong, Y., Qin, Y., Ao, X., & Li, Z. (2024). Secure Digital Asset Transactions: Integrating Distributed Ledger Technology with Safe AI Mechanisms. Academic Journal of Science and Technology, 9(3), 156-161.

[12] Zhou, Hong, et al. "Application of Conversational Intelligent Reporting System Based on Artificial Intelligence and Large Language Models." Journal of Theory and Practice of Engineering Science 4.03 (2024): 176-182.

[13] Wang, Yufu, et al. "Cloud Computing for Large-Scale Resource Computation and Storage in Machine Learning." Journal of Theory and Practice of Engineering Science 4.03 (2024).

[14] Su, Guangze, et al. "The Utilization of Homomorphic Encryption Technology Grounded on Artificial Intelligence for Privacy Preservation." International Journal of Computer Science and Information Technology 2.1 (2024): 52-58.

[15] Lin, Luqi, et al. "AI-driven Protein Engineering for DNA Sequence Modification." Journal of Theory and Practice of Engineering Science 4.03 (2024): 183-190.

[16] Cai, Guoqing, et al. "Deep Learning-Based Recognition and Visualization of Human Motion Behavior." Academic Journal of Science and Technology 10.1 (2024): 50-55.

[17] Zheng, Haotian, et al. "Medication Recommendation System Based on Natural Language Processing for Patient Emotion Analysis." Academic Journal of Science and Technology 10.1 (2024): 62-68.

[18] Wang, Hongbo, et al. "Intelligent Security Detection and Defense in Operating Systems Based on Deep Learning." International Journal of Computer Science and Information Technology 2.1 (2024): 359-367.

[19] Huang, Zengyi, et al. "Research on Generative Artificial Intelligence for Virtual Financial Robo-Advisor." Academic Journal of Science and Technology 10.1 (2024): 74-80.

[20] Xu, Jinxin, et al. "Predict and Optimize Financial Services Risk Using AI-driven Technology." Academic Journal of Science and Technology 10.1 (2024): 299-304.

[21] Huang, Zengyi, et al. "Application of Machine Learning-Based K-Means Clustering for Financial Fraud Detection." Academic Journal of Science and Technology 10.1 (2024): 33-39.

[22] Huang, Jiaxin, et al. "Enhancing Essay Scoring with Adversarial Weights Perturbation and Metric-specific AttentionPooling." 2023 International Conference on Information Network and Computer Communications (INCC). IEEE, 2023.