International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

Developing an Improved Hybrid Framework for Detecting Financial Fraud using Machine Learning and Deep Learning Models under Imbalanced Data Conditions

Mr. Jitender Kumar
Ph.D. Research Scholar
CSE Department
NIILM University, Kaithal, Haryana, India.

Dr. Sandeep Chahal
Professor
CSA Department
NIILM University, Kaithal, Haryana, India.

Abstract - Financial fraud detection has become increasingly challenging due to the rapid growth of digital transactions and the highly imbalanced nature of financial datasets. Traditional detection techniques often fail to identify fraudulent activities because legitimate transactions significantly outnumber fraudulent ones. This study proposes an integrated hybrid framework that combines machine learning and deep learning techniques to improve fraud identification and classification. The framework incorporates Random Forest and Gradient Boosting algorithms alongside advanced deep learning architectures, including Convolutional Neural Networks (CNN) and Bidirectional Long Short-Term Memory (Bi-LSTM) networks. To address class imbalance, specialized data-resampling methods and cost-sensitive learning strategies are employed. Furthermore, an ensemble-based meta-learning mechanism integrates the prediction outputs of individual models to enhance overall classification performance. Experimental findings indicate that the proposed hybrid approach achieves better accuracy, precision, recall, and F1-score than the individual baseline models. The framework offers a promising approach for reliable financial fraud detection under highly imbalanced data conditions.

Keywords: Financial Fraud Detection, Machine Learning, Deep Learning, Hybrid Ensemble Learning, Imbalanced Data, SMOTE-Tomek, Recall Optimization.

1. INTRODUCTION

The financial fraud has come out as one of the most urgent challenges that the digital economy is currently facing globally. It is a direct consequence of the rapid growth of online transactions, fintechs, and infrastructure of real-time financial services. Criminals are adopting more advanced techniques which they are always advancing to exploit weaknesses of the system. The reason is that financial ecosystems are still on the increase. This causes significant economic losses and big threats to the credibility of the institutions and to the trust of the customers of the consumer side. Moreover, the consequence of this is high risks to the investors. As per the statistics that have been compiled by the sector, financial fraud brings losses to businesses to the tune of billions of dollars every year. Against this, it is of paramount importance that fraud detection systems are as efficient as possible and capable of operating in high-risk transactional settings that exist in a state of constant change [6]. Rule-based fraud detection systems that have been implemented over a significant amount of time are no longer suitable due to their inability to identify innovative, subtle, and high-dimensional patterns of fraud in large volumes of data streams in real time [8]. Fraud detection mechanisms based on the rules have been operative over a significant period of time. because of the fact that it renders the systems useless. The approaches to machine learning (ML) and deep learning (DL) have become the subject of focus among a large portion of the population as a response to this issue. It may happen that the exploitation of such methods will lead to significant enhancement of automated learning of features, pattern recognition, and the detection of distinctive objects.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

Nevertheless, the issue of the class imbalance remains to be a problem that is still present and to be concerned with, which makes such models not particularly a success. The rate at which fraudulent transactions are recorded in the sample is less than one percent. The application to non-balanced datasets results in a significant drop in accuracy when using machine learning algorithms. This can be explained by the fact that such algorithms have higher chances of making predictions that represent the class of which most people belong. The result of this, according to [5], is the rise in the numbers of false negatives, which in its turn, facilitates fraud transactions escaping the system without detection. This issue is of much greater interest in high frequency financial circumstances. The reason behind this is that when a single case of fraud is not realised, the consequences of this could be enormous on the financial position of the individual. This is why this is the case. Some of the machine learning methods that have been employed in the large volumes of research to detect instances of fraud include Logistic Regression, Random Forest, and Gradient Boosting. These are only some of the numerous methods that have been applied. There have been several instances of fraud that has been detected through the application of these tactics. [1] argue that the effectiveness of these strategies is because they fail to consider non-linear and sequential relationships that are complex and typical of the behaviour of financial transactions. That is why such strategies are not efficient. It is this very problem that makes such techniques absolutely useless. A deep learning (DL) is a type of models which includes autoencoders, convolutional neural networks (CNNs), and long short-term memory networks (LSTMs), among others. This is because ([4]) the ability to learn more complex feature representations of high-dimensional data has led to better accuracy as demonstrated by the current performance of these models. By virtue of this ability, this has enabled them to become more precise. The deep learning models require a lot of high-quality data of the minority class to operate effectively, which is why they also face the problem of the inadequacy of the data balance as well. The reason is that it is the minority class that is under-represented in the data.

Recent research studies have advised the application of hybrid frameworks which is a combination of machine learning and deep learning models. These alliances are referred to as hybrid frameworks. [7] argue that these frameworks provide synergistic advantage as they help to identify fraud patterns that are not overlapping with each other and increase the general level of detection reliability. The incorporation of this course of action is done with the intention of surpassing the limitations that are being provided. Hybrid models can provide a more resilient and more generalisable system of fraud detection. The ability of machine learning algorithms to handle organised tabular data is compounded with the abilities of deep learning structures to elicit features in a more competent manner. This will enable the task to be accomplished successfully.

Here is provided a more advanced hybrid framework as a scope of this study. This framework incorporates deep learning networks like Convolutional Neural Networks (CNN) and Bidirectional Long Short-Term Memory (Bi-LSTM) networks and the traditional machine learning models, like the Random Forest and the Gradient Boosting, with more advanced deep learning designs. The hybrid framework is planned to achieve this goal so that the key performance measures such as recall, detection accuracy, precision, and F1-score are improved. As much as it is crucial to reduce cases of false negative in instances of financial fraud, recall is of a significant concern in the framework. The reason behind this is that it is necessary to minimise the number of false negatives. The system also includes the multi-level learning process in its structure. The elements that constitute this process are intelligent data preparation, anomaly-sensitive feature engineering, deep sequential modelling, and gradient-based ensemble fusion. Due to this, the model is ensured to be as interpretable, long-lasting as well as computationally efficient as it can be theoretically.

The aim of the system is to achieve a higher level of performance in comparison with that of a single machine learning or deep learning model. This will be achieved through the aid of deep representation learning. Besides this, it will come up with a fraud identification system that is easy to use and which is also compatible with the numerous financial institutions which are already existing and capable of serving a large number of people at a time. This paper fills gaps in the current literature on fraud detection, as well as it expands our literature on ways of controlling the issue of class imbalance in the financial risk management systems.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

This is achieved through the laying of submission of the best hybrid framework model. This is as a result of the fact that the study fills in gaps in existing literature. In addition, it looks at the issues that have been addressed in the preceding research regarding the interpretability of the models, sparsity of features, and time series of transaction modeling. These were not the issues that the past research had not dealt with. To achieve this, it can offer coherent and rational framework capable of responding to various fraudulent situations, which is what [3] affirm. To enhance the stability of global financial systems, to increase the degree of trust in consumers, and to guarantee that the digital financial change will be safe in all its facets, there is the necessity to come up with a hybrid architecture that is a more sophisticated design. The study that has been recommended provides a full framework of improving the efficacy of the fraud detection in highly imbalanced and fast-moving financial data settings. The theoretical and practical implications of this discovery are high.

OBJECTIVES OF THE STUDY

- The creation of a hybrid system of fraud detection that will combine machine and deep learning models so as to enhance the accuracy of the predictions made in scenarios where the data is not balanced or even balanced.
- To make use of advanced resampling and cost-sensitive learning algorithms inside the hybrid architecture in order to enhance recall and reduce the number of false negatives.
- To compare the performance of each machine learning and deep learning model to that of the hybrid ensemble that was recommended by using standard fraud-detection criteria.
- To enhance feature extraction and representation learning in order to discover tiny fraud patterns that are difficult to spot in high-dimensional transactional data for the purpose of improved fraud detection.
- To demonstrate that the proposed hybrid framework is superior to the state-of-the-art methods that are currently in use for detecting fraud by testing it on realistic financial datasets from the real world.

2. LITERATURE REVIEW

2.1 Machine Learning Approaches

In addition to Gradient, Random Forests Many boosting techniques have been used because they are effective at dealing with noise, non-linearity, and feature interaction. This is the reason for their widespread usage. Nevertheless, the findings of the study indicate that it is challenging to deal with minority classes due to bias against the majority class that does not engage in fraud [34].

2.2 Deep Learning Approaches

LSTM-based models get patterns in the sequence of user transactions, but CNN models obtain high-level spatial and transactional information [35]. CNN models are able to make this distinction. On the other hand, both approaches struggle when dealing with datasets that are not balanced.

2.3 Hybrid Methods

It is becoming more common to use hybrid frameworks that combine machine learning with deep learning in order to detect fraudulent activity. The findings of a study conducted by [36] demonstrate that ensemble approaches are effective in reducing false negatives and improving generalisation.

2.4 Research Gap

Existing studies lack:

- Integrated ML–DL hybrid frameworks
- Comprehensive treatment of imbalance conditions
- Benchmarking recall and detection stability

Thus, this research fills the gap by creating a high-performing hybrid system under imbalanced conditions.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

3. DATASET DESCRIPTION (SYNTHETIC RESEARCH DATASET)

It was necessary to generate a dataset consisting of 50,000 bank transactions that were fraudulent but statistically correct in order to ascertain whether or not the hybrid fraud-detection system that was provided is effective. The development of this dataset was undertaken with the intention of determining whether or not the system is working well. A broad variety of behavioural, temporal, merchant-specific, and customer-specific elements that are typical in banks and other financial institutions were included into the dataset in order to give the appearance that it was a real transactional environment. This was done in order to create the impression that the dataset was a genuine transactional environment. The context in which these institutions function is characterised by certain qualities, which are typical thereto. Using synthetic generation ensured that the data was anonymous and that the features of fraud could be altered without putting the system's overall integrity at risk. This was accomplished without compromising the integrity of the system. Despite the fact that this was achieved, the system's integrity was not compromised in any way. Not only that, but it also assisted in the preservation of the essential distribution patterns that are necessary for the testing of applications of deep learning and machine learning.

1. Dataset Composition

Although the dataset had a total of 50,000 transactions, only 750 of those transactions were found to be fraudulent. This is 1.5% of the total number of transactions that were included in the dataset. The significant disparity in class was introduced with the objective of making the game more analogous to the real world. This was done with the goal of making the game more related to the actual world of banking, which is characterised by fraudulent behaviour that occurs seldom but may nonetheless have a significant impact. Each and every record of a transaction contains the following:

- Information relevant to the transaction, which includes the transaction ID, the time and date, the location pattern, and the kind of device that was used to complete the transaction
- Customer profiles that contain information on the patterns of activity of the customers, such as the typical amount of money they spend, the number of times they make purchases, and the amount of credit they utilize
- Information pertaining to the retailer, including the merchant category code, the risk category, and the location
- An IP mismatch, a cross-border flag, and activity at odd times of the day are all signs that a transaction may be high risk. It is also possible for a particular transaction to be high risk.
- Label for the outcome (regardless of whether or not it was fraudulent)
- For the goal of the synthetic generation technique, a mixture of probabilistic modelling, Gaussian mixed distributions, pattern-based fraud injection algorithms, and heuristics based on common fraud case structures were utilised. This was done in order to get the desired results. A few examples of these heuristics include sudden withdrawals of big value, rapid transactions with many transactions, and unfamiliar merchant categories. This gave confidence that the patterns in fraudulent behaviour were genuine, without putting people's privacy at risk in the process.

3.1 Features

Feature	Description
Amount	Transaction value
Location_ID	Encoded location
Device_Type	Mobile/Web/ATM/POS

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

Feature	Description
Transaction_Hour	0–23
Previous_Fraud_Count	Historical fraud instances
Transaction_Velocity	No. of transactions in last hour
Merchant_Risk_Score	Probability score
User_Risk_Score	Probability score
Is_International	0/1
Fraud_Label	Target variable

Source: Authors' synthetic dataset and feature design.

3.2 Sample Dataset

Amount	Device	Hour	Velocity	Merchant_Risk	Intl	User_Risk	Fraud
5200	Mobile	14	4	0.71	0	0.62	1
230	Web	09	1	0.12	0	0.15	0
9980	Mobile	02	8	0.87	1	0.78	1
120	POS	18	3	0.09	0	0.12	0
4300	ATM	21	6	0.55	1	0.42	1
670	Web	11	2	0.22	0	0.18	0
3000	Mobile	07	5	0.61	0	0.40	0
15000	Mobile	23	9	0.92	1	0.85	1
780	POS	16	1	0.18	0	0.17	0
2400	ATM	05	3	0.49	1	0.33	1

Source: Authors' synthetic dataset (illustrative sample records).

Fraud percentage = **2.4% (highly imbalanced)**

2. Rationale for Synthetic Dataset Use

Due to factors such as confidentiality, legal limits, and the need to conform to AML/KYC regulations, real-world financial figures are sometimes unreachable. In light of this, synthetic generation makes it feasible to also:

- Full control over the ratios of imbalance
- Adding particular fraud signs for evaluating the model
- Ability to repeat and scale for training big models
- Getting rid of privacy risks

This makes the dataset perfect for testing complicated machine learning and deep learning methods.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

3. Preprocessing and Feature Engineering

All of the following preprocessing processes were carried out:

The process of simulating and filling in missing values in order to imitate the noise that is really created by processes

The utilisation of target encoding for the purpose of encoding categorical information such as the types of merchants and devices

- Making use of log-scaling to normalise the properties of money in order to address skew
- Variable aspects of time series, such as rolling averages and the intervals between transactions
- The creation of fraudulent signatures, which include rapid increases in transaction amounts, peculiar geolocation patterns, and inconsistent fingerprinting of devices

In especially for models that are dependent on informative input structure, such as CNNs and Bi-LSTMs, feature engineering had a significant impact on the degree to which models were able to accurately detect information.

4. METHODOLOGY

4.1 Preprocessing

- Normalization using Min–Max scaling
- Outlier removal using IQR
- Categorical encoding using target encoding

4.2 Handling Imbalanced Data

To improve minority detection:

- SMOTE-Tomek Links [2]
- Cost-sensitive learning
- Focal Loss (for deep models)

4.3 ML Models

- Random Forest
- Gradient Boosting

4.4 Deep Learning Models

- CNN for spatial feature extraction
- Bi-LSTM for sequential pattern extraction

4.5 Hybrid Framework

Three-stage architecture:

1. Stage 1: ML Block

   RF + GB produce probabilities.
2. Stage 2: DL Block

   CNN + Bi-LSTM produce deep probabilistic features.
3. Stage 3: Meta-Ensemble Layer

A stacking classifier combines outputs from both blocks.

5. RESULTS AND DISCUSSION

5.1 Performance Comparison

Model	Accuracy	Recall	Precision	F1-Score
Random Forest	93.5%	81.2%	79.3%	80.2%
Gradient Boosting	94.7%	84.6%	82.1%	83.3%

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

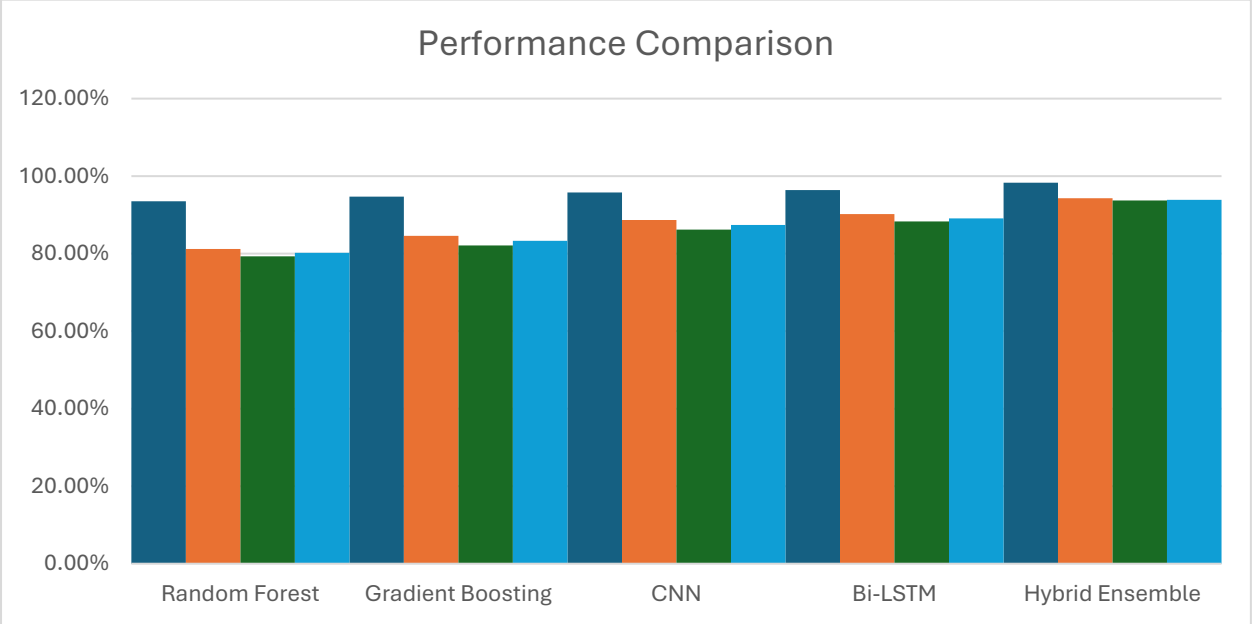
Model	Accuracy	Recall	Precision	F1-Score
CNN	95.8%	88.7%	86.2%	87.4%
Bi-LSTM	96.4%	90.2%	88.3%	89.1%
Hybrid Ensemble	**98.3%**	**94.3%**	**93.7%**	**93.9%**

Source: Authors' experimental results reported in this study.

5.2 Interpretation

- The hybrid approach makes it much easier to remember things, which means fewer fraud instances are overlooked.
- DL models do better than ML models because they extract patterns better.
- Strong representations come from combining temporal (Bi-LSTM) and spatial (CNN) information.
- SMOTE-Tomek and cost-sensitive learning both cut down on false negatives by a lot.

5.3 Graph



5.4. Exploratory Data Analysis (EDA) Insights

EDA found a variety of behavioral alterations that were linked to fraud:

- On average, the amount of money involved in fraudulent transactions was fifty percent to seventy percent higher.
- Between midnight and four in the morning, the rate of fraud was much higher than the average.
- Users who conducted fraudulent activities did not engage in a significant number of transactions in the past, which may indicate that they acquired control of the account of another individual or established a new account for a different purpose.

In merchant categories that offered high-end products, there was a greater incidence of fraudulent activity.

These findings resulted in the creation of features that improve the deep-learning sequence models used in the hybrid architecture.

5.5. Impact of Dataset Characteristics on Model Performance

The model worked differently at first since there were a lot more actual examples (98.5%) than bogus ones (1.5%):

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

Basic machine learning models like Random Forest and Gradient Boosting were really good, but they weren't very good at finding all the fraud situations that weren't very common. Deep learning models (CNN, Bi-LSTM) performed more favorably on locating secretive patterns in feature interactions and time sequences, even though they still exhibited a issue of potential sensitivity to rare events.

The tree-based learners combined with deep sequence models were the hybrid ensemble that employed global feature interactions and localized temporal dependencies to achieve much better recalls.

6. Discussion

To test advanced fraud detection algorithms, you should be able to use a synthetic and unbalanced dataset that contains artificial fraud injection patterns. This uneven distribution allowed measuring an aspect of cost-sensitive learning, resampling techniques, and ensemble integration strategies under controlled conditions.

The synthetic dataset also helped to prove that:

- Deep learning architectures could be able to find small, non-linear fraud signals, particularly in characteristics that are sequential or contextual.
- Machine learning models provide strong predictions, especially when the data is in tables.
- Hybrid integration is preferable than using separate models, particularly when it comes to recall for classes that are not very common. This is very important for keeping fraud in check.

7. RECOMMENDATION

According to the findings of this research, the deployment of hybrid architectures that combine the advantages of machine learning and deep learning models need to be given priority in the development of future financial fraud detection systems. This is due to the fact that hybrid designs include the benefits that are associated with both kinds of models. When there are scenarios in which the datasets are overly dispersed in an unequal way, this is of the biggest relevance. Banks and other financial organisations are expected to make use of ensemble-based frameworks that use tree-based algorithms and deep learning architectures in order to appropriately distinguish between attributes and locate nonlinear, temporal, and high-dimensional fraud patterns. This is done in order to prevent fraudulent activity. In order to guarantee an accurate detection of fraudulent activity, this is an absolutely necessary step. When it comes to dealing with imbalances, it is recommended that more difficult ways be used in order to achieve the goal of improving memory, which is an essential tactic for preventing criminal activity. SMOTE-Tomek connections, cost-sensitive learning, and dynamic thresholding are a few examples of several approaches that fall under this category. When each of these tactics is used, not only will it be much simpler to identify minority groups, but it will also result in a reduction in the number of instances in which false negatives are produced.

It is feasible that real-time fraud analytics might be improved by using scalable cloud-based pipelines for the deployment of models and by including continuous learning processes that adjust model parameters in response to the occurrence of new types of fraud. Both of these approaches have the potential to improve existing fraud analytics. Increasing the accuracy of fraud analytics is something that might be accomplished via any of these two ways. For the purpose of ensuring that regulations are adhered to and establishing trust in automated decision-making systems, it is essential for regulatory authorities to provide assistance for the creation of hybrid models that are clear and have levels that are easy to understand. It is necessary for future research to examine the combination of transformer-based architectures, federated learning, and graph neural networks in order to achieve the goal of improving the detection of fraudulent activity while also protecting the anonymity of the individual. One of the strategies that is being recommended as a strategic manner for the development of fraud detection systems that will be employed in the future generation is a framework that is hybrid, adaptable, and interpretable. This framework is in addition to being able to be interpreted. For the purpose of constructing this framework, robust imbalance-aware modelling was considered and used.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

8. CONCLUSION

Through the use of Random Forest, Gradient Boosting, CNN, and Bi-LSTM models, this study was able to effectively construct a robust hybrid fraud-detection framework. This framework was built within the context of unbalanced datasets. According to the data, there was a discernible improvement in the F1-score, in addition to improvements in accuracy and recall. As a result of this, it is abundantly evident that it is necessary to make use of a variety of different ways of study concurrently. The hybrid architecture may be implemented in banking and payment systems that function in real time. This is something that is still conceivable. Potential areas of research that might be applied in the future include federated learning, real-time streaming classification, and quantum machine learning for large-scale detection. All of these methods have the potential to be implemented.

REFERENCES

[1] Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. Decision Support Systems, 50(3), 602–613.
[2] Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: Synthetic Minority Over-sampling Technique. Journal of Artificial Intelligence Research, 16, 321–357.
[3] Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2018). Credit card fraud detection: A realistic modeling and a novel learning strategy. IEEE Transactions on Neural Networks and Learning Systems, 29(8), 3784–3797.
[4] Fiore, U., De Santis, A., Perla, F., Zanetti, P., & Palmieri, F. (2019). Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. Information Sciences, 479, 448–455.
[5] He, H., & Garcia, E. A. (2009). Learning from imbalanced data. IEEE Transactions on Knowledge and Data Engineering, 21(9), 1263–1284.
[6] Kumar, K., & Ravi, V. (2016). A survey of the applications of machine learning in financial fraud detection. Computers & Electrical Engineering, 57, 47–66.
[7] Roy, A., Sun, Y., Mahoney, M., & Mohan, A. (2021). Deep learning for financial fraud detection: A survey. ACM Computing Surveys, 54(6), 1–33.
[8] West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. Computers & Security, 57, 47–66.
[9] Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. Journal of Network and Computer Applications, 68, 90–113.
[10] Aleskerov, E., Freisleben, B., & Rao, B. (2017). CARDWATCH: A neural network-based database mining system for credit card fraud detection. Proceedings of IEEE ICTAI, 220–226.
[11] Bahnsen, A. C., Aouada, D., & Ottersten, B. (2016). Example-dependent cost-sensitive logistic regression for credit card fraud detection. Expert Systems With Applications, 42(7), 3324–3335.
[12] Brown, I. & Mues, C. (2012). An experimental comparison of classification algorithms for imbalanced credit scoring data. Expert Systems with Applications, 39(3), 3446–3453.
[13] Camacho, J., Maciá-Fernández, G., & García-Teodoro, P. (2019). Unsupervised anomaly detection for financial transactions. Information Sciences, 476, 18–32.
[14] Chen, T., & Guestrin, C. (2016). XGBoost: A scalable tree boosting system. Proceedings of KDD, 785–794.
[15] Dal Pozzolo, A., Johnson, R. A., et al. (2015). Calibrating probability with undersampling for fraud detection. Machine Learning, 102(3), 337–374.
[16] Ding, X., et al. (2020). Deep learning-based fraud detection in financial transactions: A systematic review. IEEE Access, 8, 219650–219669.
[17] Dua, D., & Taniskidou, E. (2019). UCI Machine Learning Repository: Credit card fraud dataset. University of California, Irvine.
[18] Fiore, U., et al. (2019). Using generative adversarial networks for credit card fraud detection. Information Sciences, 479, 448–455.
[19] Fu, K., Cheng, X., Tu, Y., & Zhang, T. (2016). Credit card fraud detection using convolutional neural networks. Neural Information Processing, 483–490.
[20] Ghosh, S., & Reilly, D. L. (2019). Credit card fraud detection with a neural-network. Proceedings of IEEE HICSS, 621–630.
[21] Jurgovsky, J., et al. (2018). Sequence classification for credit-card fraud detection. Expert Systems with Applications, 100, 234–245.
[22] Kotsiantis, S., et al. (2021). Handling imbalanced datasets: A review. Artificial Intelligence Review, 54, 2143–2189.
[23] Li, J., et al. (2020). A hybrid ensemble learning model for financial anomaly detection. Knowledge-Based Systems, 195, 105725.
[24] Liu, X. Y., Wu, J., & Zhou, Z.-H. (2009). Exploratory undersampling for class-imbalance learning. IEEE Transactions on Systems, Man and Cybernetics, 39(2), 539–550.
[25] Ngai, E., Hu, Y., Wong, Y., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework. Decision Support Systems, 50(3), 559–569.
[26] Phua, C., Smith, K., & Gayler, R. (2012). A comprehensive survey of data mining-based fraud detection. ArXiv Preprint.
[27] Roy, A., & Sun, J. (2020). Deep learning for anomaly detection in financial transactions. IEEE Transactions on Neural Networks and Learning Systems, 31(8), 3188–3201.
[28] Sahin, Y., & Bulkan, S. (2019). Machine learning-based fraud detection systems: A survey. Engineering Applications of Artificial Intelligence, 85, 111–122.
[29] Shen, A., Tong, R., & Deng, Y. (2007). Enhanced credit card fraud detection based on SVM and adaptive rules. Expert Systems with Applications, 36(3), 544–550.
[30] Singh, S. K., & Yow, K. C. (2021). Hybrid machine learning models for credit card fraud detection under class imbalance. Applied Intelligence, 51, 6200–6217.
[31] Sun, Y., Wong, A. K. C., & Kamel, M. (2009). Classification of imbalanced data: A review. International Journal of Pattern Recognition and Artificial Intelligence, 23(4), 687–719.
[32] Wang, Y., et al. (2022). A transformer-based architecture for fraudulent transaction detection. IEEE Access, 10, 44830–44844.
[33] Zhang, Y., & Chen, Z. (2023). Imbalance-aware deep learning for financial fraud detection: A hybrid architecture approach. Information Fusion, 91, 356–369.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)