iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: IX Month of publication: September 2025

DOI: https://doi.org/10.22214/ijraset.2025.74246

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IX Sep 2025- Available at www.ijraset.com

A Survey on Advanced Fraud Detection: Leveraging K-SMOTEENN and Stacking Ensemble to Tackle Data Imbalance and Extract Insights

Vyshnavi M[1], Chaithra M[2], Dhanya Shetty[3], Nireeksha Pai B N[4]
[1]*Assistant Professor, Dept of CSE, Sapthagiri College of Engineering*
[2, 3, 4]*Dept of CSE, Sapthagiri College of Engineering*

Abstract: DCCF is a major problem for financial security because the datasets are very uneven and fraudulent activities are becoming more and more sophisticated. To solve these problems, a new detection framework is made by combining k-means SMOTEENN with a stacking ensemble of ML algorithms. The dataset, which has a lot of class imbalance and contains anonymised transaction records, is preprocessed and balanced using k-means SMOTEENN. This method oversamples instances from the minority class while getting rid of noisy synthetic samples, which lowers the chance of overfitting. A stacking ensemble is built on this balanced dataset by combining different classifiers like XGBoost, decision Tree, and other base learners. A meta-learner then combines their outputs to make a strong decision boundary. The experimental findings show that this model works far better than standalone classifiers, "with an F1-score of 0.92, a precision of 0.95, a recall of 0.88, an area under the precision-recall curve (AUPRC) of 0.96, and a perfect ROC-AUC of 1.00. To make dependability even better, Explainable AI (XAI) methods are used. for example, local Interpretable model-Agnostic explanations (LIME)" show how important features affect the model and explain the roles of base and meta-learners. This guarantees both high detection accuracy and ease of understanding, making it possible to find fraud safely and clearly in real-world financial settings.

"Index Terms: K-MEANS, SMOTEENN, credit card, fraud detection, stacking ensemble, imbalance Technique".

I. INTRODUCTION

The rapid growth of financial transactions in recent years has been mainly caused by the growth of banks and the growing use of online shopping sites. This increase shows how digital payment systems are becoming more common and how the world is moving toward doing business online [1]. Although these have made things easier and more accessible, it has also created new avenues where people have gone out of their way to cheat especially in transactions involving credit cards. Cards, in particular, have become one of the most significant concerns of both customers and financial institutions due to fraud. It tells the economy and security big problems [2].

History demonstrates that this situation is becoming increasingly worse. Indicatively, approximately 21.84 billion was impaired due to credit card fraud in 2015. In 2019, this figure had significantly increased to 28.65 billion, a very alarming increase in only four years [2]. According to the Nilson Report, credit card theft continues to increase, and it is projected that losses "will increase not only to $18.11 billion in 2014 but also to $43.47 billion by 2028 [3]". In 2016, the highest rate of fraud per 100 spent on transactions was 7.2 cents, which is the highest point ever recorded. It will be estimated to fall to 6.4 cents in 2028. Nevertheless, the general price of fraud is rather high [3]. This paradox explains why there is a necessity to develop better detection methods that can keep pace with changing and more sophisticated methods of fraud.

Traditional fraud detection methods, which generally use human rules, threshold-based systems, or simple statistical models, are not enough to stop modern, large-scale fraud attempts [4]. Fraudsters are always changing by using new technology to get around traditional detection methods, using advanced evasion techniques, and finding vulnerabilities in transaction systems [5]. This fast-paced world needs frameworks based on ML and DL that can understand complex patterns, find strange things, and find fraud with a high degree of accuracy [6].

Among the key issues of relying on ML models to identify fraud is the presence of the class imbalance issue that occurs when few transactions among many are fraudulent [7]. This asymmetry usually leads to biases of classifiers in the majority (legal) transactions, making it more difficult to discover unusual but valuable fraudulent events. As a solution to this issue, novel resampling algorithms such as K-SMOTEENN have been proposed to equalize datasets through smartly oversampling the minority groups and eliminating noise and edge cases [8]. Such approaches are compatible with ML approaches, and in particular with stacking ensembles, which fuse the properties of multiple classifiers. This renders them effective in developing fraud detection systems which are robust, scalable, and high-performing.

II. LITERATURE REVIEW

Detection of CCF has become a critical area of study in the field of financial cybersecurity, and it now attracts significant attention in the academic and industrial circles, as the level of sophistication of fraudulent schemes and the size of digital transactions continue to grow. An in-depth review of the existing literature reveals the gradual shift toward complex ML and DL models and scholars focusing on the solutions to the following challenges: the uneven distribution of data, noise in data, and the ability to scale models.

A comprehensive research on the methodologies of credit card cyber fraud detection using ML and DL techniques "was carried out by E. A. L. Marazqah Btoush, X. Zhou, R. Gururajan, K. C. Chan, R. Genrich and P. Sankaran [9]". Their study incorporated new concepts combining various classifiers, ensemble methods, and hybrid approaches, as well as emphasising the current problem of data imbalance in fraud detection work. The review not only pointed out the flaws in traditional models, but it also proposed that future research should look into hybrid frameworks that mix sampling methods with more complex ensemble classifiers. The authors emphasized the significance of precision and recall as more dependable measurements than accuracy, due to the extremely skewed characteristics of fraud datasets, by examining a diverse range of models.

Based on ensemble "methods, M. A. Mim, N. Majadi, and P. Mazumder [10]" came up with a soft voting ensemble learning method for finding CCF. Their approach combines several basic classifiers using a single voting system to improve accuracy and reliability. The research indicated that ensemble learning surpassed individual models in identifying varied fraud patterns and minimizing false negatives, which are especially detrimental in financial contexts. By using the strengths of several classifiers, the authors proved that the ensemble approach could give the same results on diverse datasets. This shows that ensemble tactics are still important in research on fraud detection.

Researchers have also looked into random forest classifiers a lot because they are easy to understand and work well even when there is noise. "M. H. Aung, P. T. Seluka, J. T. R. Fuata, M. J. Tikoisuva, M. S. Cabealawa, and R. Nand [11]" studied the use of a random forest classifier in the detection of CCF based on the use of performance indicators. Their results also showed that random forest was able to effectively handle high-dimensional data, and it provided competitive results in comparison to traditional classifiers. Instead, the authors acknowledged that imbalanced datasets were not without their own issues and tended to produce biased categorization outcomes favoring real transactions. Their solution to these issues was to resort to resampling and enhancement of feature engineering.

Based on this study, A. M. Aburbeian and H. I. Ashqar [12] produced a better random forest classifier that can be used to detect a credit card fraud in unbalanced data. They also used the oversampling and feature selection methods in their architecture to minimize the dominance of dominant classes that could easily identify the fake transactions. The authors demonstrated the superiority of their approach to the traditional random forest models when tested on benchmark datasets. It was more precise, recalled, and F1. They found that the effectiveness of tuning base classifiers using customized preprocessing methods supported the effectiveness of morphing base classifiers to support skewness in real-world fraud data.

Another valuable addition to unbalanced learning was achieved by "H. Zhu, M. Zhou, G. Liu, Y. Xie, S. Liu and C. Guo [13], who developed the so-called Noisy Sample-Removed Undersampling Scheme (NUS)" to handle imbalanced classification. Their approach attempted to increase the precision of their fraud detection by removing noisy or redundant examples that belong to the majority class and thereby complicate the process of classifier learning. NUS significantly contributed to the recall of the minority class when performing credit card fraud detection tasks but did not negatively affect overall performance. The researchers noted that common undersampling methods would discard critical information in some cases, whereas NUS method retained key patterns by simply eliminating noise.

In order to address the issues of oversampling, X. Wang, J. Gong, Y. Song and J. Hu [14] developed an adaptive-weighted three-way decision oversampling technique which was founded on a cluster imbalanced-ratio mechanism.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IX Sep 2025- Available at www.ijraset.com

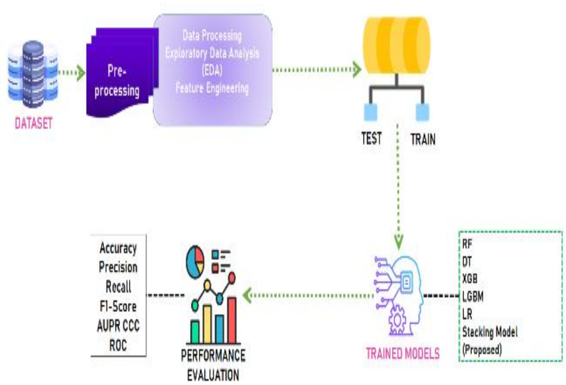
Their plan modified the oversampling weights according to the breakdown of the clusters and ensured that the minority cases of fraud were more fairly represented. Not only was this technique more accurate at detecting, but also reduced the likelihood of overfitting, which is a significant issue with the oversampling methods such as SMOTE. The authors demonstrated that their approach could be implemented on a large scale and that it can be applied to uncover fraud on a very large scale, where both speed and accuracy are of paramount importance.

Out of the earlier studies that concentrate on sampling and classifiers, the article by "A. Abd El-Naby, E. E.-D. Hemdan, and A. El-Sayed [15]" has a nice approach to detecting fraud in financial services that is effective when the credit card data is skewed. They combined both the state-of-the-art preprocessing techniques and ML classifiers in order to achieve balanced detections. The authors highlighted the issues associated with applying fraud detection technologies to real-world banks, where the vast number of false positives may spoil the client experience. Their proposed framework was centered on reaching a compromise between the two elements of security and usability by maintaining high rates of recall and reducing the number of transactions that were rejected without a proper reason.

Of significance, are the works of S. K. Hashemi, S. L. Mirtaheri and S. Greco [16] who investigated finding fraud in financial data with the help of alternative ML techniques. They tested their algorithms (DT, SVM, and ensemble) in order to compare their effectiveness in the situation with imbalanced data. The findings indicated that no single method would be effective than all the other methods in all datasets. This indicates that we should combine hybrid and ensemble-based approaches. The authors have highlighted how they need to keep on adapting as fraudsters are ever-evolving, upgrading their methods to exploit vulnerabilities within a system.

III. MATERIALS AND METHODS

The suggested system includes a strong framework for detecting CCF that can handle very uneven data and make sure that classification is accurate. The approach uses a publicly available anonymized credit card transaction dataset that has a lot of legal and fake transactions but very few of each. To fix this problem, K-means SMOTEENN is used. This method combines the cluster-based "Synthetic Minority Oversampling Technique (SMOTE) with Edited Nearest Neighbors (ENN)" to oversample instances from the minority class while getting rid of noisy or duplicate samples, which improves the quality of the data. A stacking ensemble method is used on this improved dataset, "combining different ML classifiers as XGBoost, Decision Tree, Random Forest, and Logistic Regression". These base learners identify different decision patterns, and a meta-learner combines these results to make a strong and general categorization border. The system also uses "Explainable AI (XAI) methods, such as Local Interpretable Model-Agnostic Explanations (LIME)", to make predictions easier to understand by pointing out important features that affect them and making model behavior clearer.



"Fig.1 Proposed Architecture"

The first step in the system design is to collect datasets. The next step is to preprocess the data to deal with missing values, normalize it, and change it. Data processing comprises "exploratory data analysis (EDA)" and feature engineering to make the input better. We divide the cleaned data into training and testing sets, and then we train many models on the "training set, including Random Forest (RF), Decision Tree (DT), XGBoost (XGB), LightGBM (LGBM), and Logistic Regression (LR)". A proposed stacking model combines their best features. "Finally, metrics including accuracy, precision, recall, F1-score, AUPR CCC, and ROC are used to judge performance".

A. Dataset Collection

The dataset utilized is a synthetic credit card transaction dataset produced by the PaySim simulator, which emulates actual mobile money services. It is based on transaction data from a multinational company that does business in more than 14 countries. This makes sure that the behavior patterns are accurate while keeping people's anonymity. There are more than six million records in the collection, and each one has 11 parameters, such as the kind of transaction, the amount, the account balances, the sender and receiver details, and fraud indications. Fake transactions are included to test detection algorithms, which makes it very useful for building fraud detection systems.

B. Pre-Processing

The preprocessing phase cleans, explores, engineers features, and prepares ensembles from the raw PaySim dataset. This ensures that the data is balanced, organized and helpful in creating models that can detect credit card fraud.

1) Data Processing: In the data processing stage, the PaySim data was cleaned and preprocessed to ensure that the data was of good quality to be used in training the model. Missing values were identified by the isnull() method and flagged to be corrected. The duplicated method was checked to find out whether there were any duplicates in the data and it revealed that there were no duplicates in the dataset. We also applied random sampling, removal of noise and feature selection to retain only the useful properties. This simplified the use of this dataset in modeling fraud detection.
2) Exploratory Data Analysis (EDA): We run the EDA on the PaySim dataset of 6 362,620 transactions and 11 attributes to identify patterns and relationships. This dataset exhibited the extremely uneven distribution of classes with 8,213 fraudulent transactions and almost 6.35 million valid transactions. The correlation between newbalanceOrig and oldbalanceOrig was high and, thus, one of the attributes had to be dropped. An attribute isFlaggedFraud was also removed since it did not contribute much value. The various categories of transaction were analysed and the most common ones were cash-out and payment. This knowledge is quite helpful to model fraud detection.
3) Feature Engineering: Feature engineering was done to enhance the features of the data with some useful attributes. The variables of origin and destination were combined to form another feature named type2. This feature is used to economize transactional interactions by logical encoding, namely, CC, CM, MC, and MM. In order to clear things further, the original characteristics were changed into other names and were later deleted after the change. The method simplified the dataset, as it was no longer in two dimensions but one. This improved the functionality of the model and made the trends more visible, such as the fact that transactions between customers and customers are more prevalent.

C. Training and Testing

In order to develop and test the fraud detection model, the dataset was divided into two: training and testing. We trained K-SMOTEENN to equalize the training set and then used the training set to teach a few base learners in the stacking ensemble how to distinguish between real and fake transactions. The learners at the bottom were then tasked with predicting and the predictions were forwarded to a meta-learner that combined the outputs to produce a robust final model. The separate testing set was to test the ability of the model to work well on data it had not encountered before to ensure it could be applied to another scenario and was accurate.

D. Algorithms

1) XGBoost: XGBoost is selected because it is an efficient gradient boosting model that can provide support even to transaction data that are not distributed uniformly. It identifies complex relationships and occurrences of characteristics, thereby simplifying the identification of untrue transactions and reducing overfitting by the regularization and boosting techniques.
2) Decision Tree: Decision tree is a rule based classification tool that divides the data by feature decisions to answer the question of whether the transaction is real or fake. It facilitates the discovery of important trends within transactions and belongs to the stacking collection that strengthens the model as a whole and makes it more precise.
3) Random Forest: The combination of a few decision trees to make the model broader and less variable is known as Random Forest. It relies on bootstrapped samples and random features in order to discover fraud trends in datasets that are not balanced in order to contribute a variety of predictions to the ensemble model.
4) Logistic Regression: Logistic regression is an algorithm based on a linear combination of features that predicts the probability of a transaction to be a fake one. It is easy to use and comprehend, and as a result it can be added to the stacking group of advanced base learners. This enhances the stability of predictions on a large scale and provides details regarding the influence of features on predictions.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IX Sep 2025- Available at www.ijraset.com

5) Stacking Ensemble: Stacking Ensemble uses a meta-learner to aggregate predictions from several base learners into a strong, broad model. It combines the best parts of many classifiers to make detection more accurate and reduce the number of false positives in the PaySim dataset.

IV. EXPERIMENTAL RESULTS

1) Accuracy: How well a test can distinguish between sick and healthy individuals determines its accuracy. We may determine a test's accuracy by comparing how well it can make this distinction. And, in all examples we have considered, we ought to measure the percentage of true positives and true negatives. In mathematics, this can be written as follows:

$$"Accuracy = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{FP} + \mathrm{TN} + \mathrm{FN}} (1)"$$

2) Precision: Precision refers to the percentage of successfully classified core cases or samples among all the cases classified as positives. So, the equation to determine the accuracy is:

$$"Precision = \frac{\text{True Positive}}{\text{True Positive } + \text{False Positive}} (2)"$$

3) Recall: In ML, recall is used to measure how well a model can locate all the pertinent examples of a particular class. The effectiveness with which a model captures all instances of a particular class is shown by the ratio of accurately predicted positive observations to the total actual positives.

$$"Recall = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}} (3)"$$

4) F1-Score: The of a ML model can be assessed using the F1 score. It combines a model's precision and recall scores. The accuracy indicator shows you how many times a model successfully predicted the entire dataset.

$$"F1\ Score = 2 * \frac{Recall \text{ X } Precision}{Recall + Precision} * 100(4)"$$

5) AUC-ROC Curve: The AUC-ROC Curve is a technique for evaluating how well a classification issue functions at various threshold levels. The True Positive Rate and False Positive Rate are displayed on the same graph by the ROC. The model's ability to distinguish between classes is measured by the AUC. The model is more effective if the AUC is higher.

$$"AUC = \sum_{i=1}^{n-1} (FPR_{i+1} - FPR_i) \cdot \frac{TPR_{i+1} + TPR_i}{2} \ (5)"$$

We look at the performance metrics for each algorithm in "Tables 1 and 2. These include accuracy, precision, recall, F1-score, AUPR CCC, and ROC. For both, the Stacking classifier gets the best scores". The tables below also show how different algorithms compare in terms of their metrics.

"Table.1 Performance Evaluation Table - without collaboration feature construction and K-SMOTEENN"

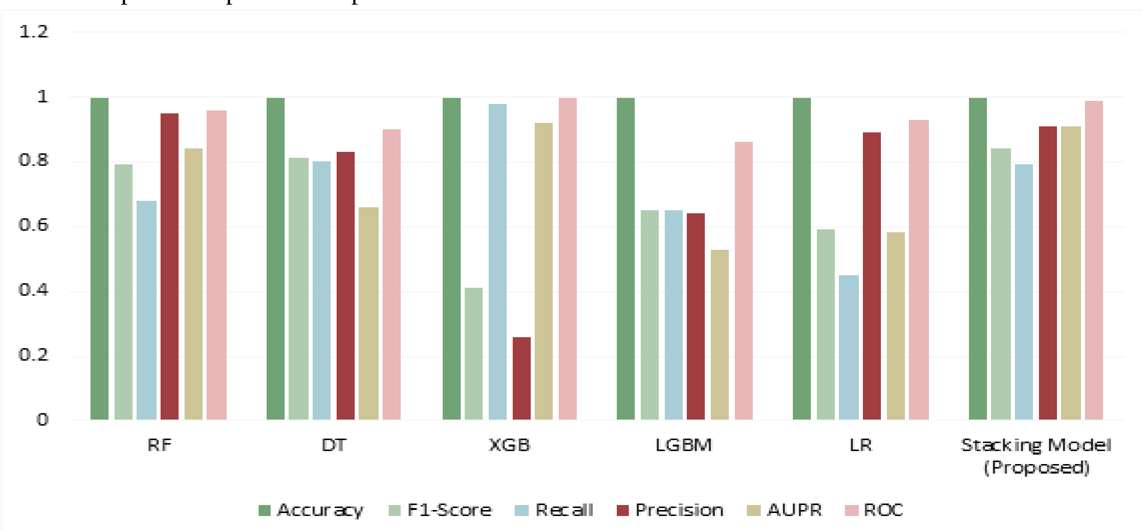
Classifier	Accuracy	F1-Score	Recall	Precision	AUPR CCC	ROC
RF	1.00	0.79	0.68	0.95	0.84	0.96
DT	1.00	0.81	0.80	0.83	0.66	0.90
XGB	1.00	0.41	0.98	0.26	0.92	1.00
LGBM	1.00	0.65	0.65	0.64	0.53	0.86
LR	1.00	0.59	0.45	0.89	0.58	0.93
Stacking Model (Proposed)	**1.00**	**0.84**	**0.79**	**0.91**	**0.91**	**0.99**

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IX Sep 2025- Available at www.ijraset.com

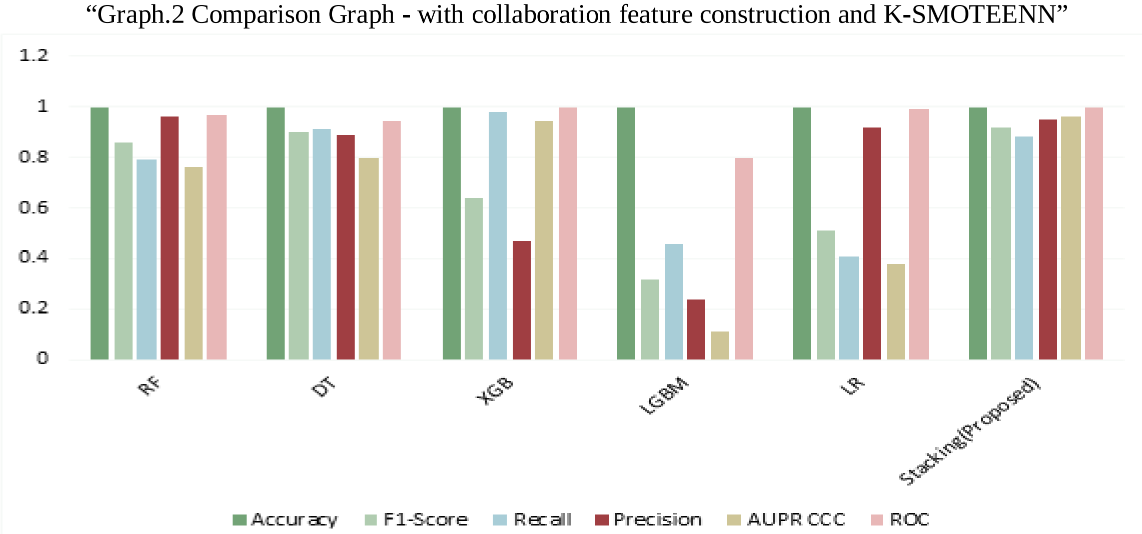
"Table.2 Performance Evaluation Table – with collaboration feature construction and K-SMOTEENN"

Classifier	Accuracy	F1-Score	Recall	Precision	AUPR CCC	ROC
RF	1.00	0.86	0.79	0.96	0.76	0.97
DT	1.00	0.90	0.91	0.89	0.80	0.94
XGB	1.00	0.64	0.98	0.47	0.94	1.00
LGBM	1.00	0.32	0.46	0.24	0.11	0.80
LR	1.00	0.51	0.41	0.92	0.38	0.99
Stacking(Proposed)	**1.00**	**0.92**	**0.88**	**0.95**	**0.96**	**1.00**

"Graph.1 Comparison Graph - without collaboration feature construction and K-SMOTEENN"



"Graph.2 Comparison Graph - with collaboration feature construction and K-SMOTEENN"



In Graphs (1 - 2), The comparison graph shows performance measures for a few models. "The metrics are accuracy (dark green), F1-score (light green), recall (blue), precision (red), AUPR/CCC (gold), and ROC (pink)". The suggested stacking model routinely gets greater balanced scores on most measures.

V. CONCLUSION

The suggested approach shows a sophisticated and successful way to find credit card fraud by dealing with the important problems of data imbalance, overfitting, and interpretability. K-means SMOTEENN is used on the very unbalanced anonymized credit card transaction dataset to improve class distribution by making synthetic samples for the minority class and filtering out noisy or duplicate data through Edited Nearest Neighbors. This improves data quality and lowers the risk of overfitting. A stacking ensemble framework is built on this balanced dataset "by combining classifiers like XGBoost, Decision Tree, Random Forest, and Logistic Regression". A meta-learner then combines the outputs of these classifiers to create a strong and general decision boundary. The experimental evaluation shows that the results are far better than those of the separate baseline classifiers. "The F1-score is 0.92, the precision is 0.95, the recall is 0.88, the AUPRC is 0.96, and the ROC-AUC is 1.00. Also, Explainable AI (XAI) methods are used, and Local Interpretable Model-Agnostic Explanations (LIME)" make things clearer by showing which features are most important for making predictions and how base and meta-learners work together. This mix of resampling approaches, ensemble algorithms, and interpretability makes for a very accurate, dependable, and clear fraud detection system that works well in real-world financial settings.

The future of this system includes improving fraud detection by adding DL models like LSTM and Transformer-based architectures to find trends in transactions over time. Adding more financial records from different sources, such as cross-border and real-time transactions, can make the dataset even more robust. Federated learning will help keep model training private between universities. Also, moving Explainable AI beyond LIME with techniques like SHAP can make it easier to understand, which will help financial companies use flexible, scalable, and clear fraud detection solutions in changing situations.

REFERENCES

[1] Mienye, I. D., & Jere, N. (2024). Deep learning for credit card fraud detection: A review of algorithms, challenges, and solutions. IEEE Access, 12, 96893–96910.
[2] Ileberi, E., Sun, Y., & Wang, Z. (2021). Performance evaluation of machine learning methods for credit card fraud detection using SMOTE and AdaBoost. IEEE Access, 9, 165286–165294.
[3] Alfaiz, N. S., & Fati, S. M. (2022). Enhanced credit card fraud detection model using machine learning. Electronics, 11(4), 662.
[4] Gupta, P., Varshney, A., Khan, M. R., Ahmed, R., Shuaib, M., & Alam, S. (2023). Unbalanced credit card fraud detection data: A machine learning-oriented comparative study of balancing techniques. Procedia Computer Science, 218, 2575–2584.
[5] Mienye, I. D., & Sun, Y. (2023). A deep learning ensemble with data resampling for credit card fraud detection. IEEE Access, 11, 30628–30638.
[6] Singh, A., Ranjan, R. K., & Tiwari, A. (2022). Credit card fraud detection under extreme imbalanced data: A comparative study of data-level algorithms. Journal of Experimental & Theoretical Artificial Intelligence, 34(4), 571–598.
[7] Khan, A. A., Chaudhari, O., & Chandra, R. (2023). A review of ensemble learning and data augmentation models for class imbalanced problems: Combination, implementation, and evaluation. Expert Systems with Applications, 244, 122778.
[8] Ni, L., Li, J., Xu, H., Wang, X., & Zhang, J. (2023). Fraud feature boosting mechanism and spiral oversampling balancing technique for credit card fraud detection. IEEE Transactions on Computational Social Systems, 11(2), 1615–1630.
[9] Marazqah Btoush, E. A. L., Zhou, X., Gururajan, R., Chan, K. C., Genrich, R., & Sankaran, P. (2023). A systematic review of literature on credit card cyber fraud detection using machine and deep learning. PeerJ Computer Science, 9, e1278.
[10] Mim, M. A., Majadi, N., & Mazumder, P. (2024). A soft voting ensemble learning approach for credit card fraud detection. Heliyon, 10(3), e25466.
[11] Aung, M. H., Seluka, P. T., Fuata, J. T. R., Tikoisuva, M. J., Cabealawa, M. S., & Nand, R. (2020). Random forest classifier for detecting credit card fraud based on performance metrics. In Proceedings of IEEE Asia–Pacific Conference on Computer Science and Data Engineering (CSDE) (pp. 1–6).
[12] Aburbeian, A. M., & Ashqar, H. I. (2023). Credit card fraud detection using enhanced random forest classifier for imbalanced data. In Proceedings of International Conference on Advanced Computing Research (pp. 605–616)
[13] Zhu, H., Zhou, M., Liu, G., Xie, Y., Liu, S., & Guo, C. (2023). NUS: Noisy sample-removed undersampling scheme for imbalanced classification and application to credit card fraud detection. IEEE Transactions on Computational Social Systems, 11(2), 1793–1804.
[14] Wang, X., Gong, J., Song, Y., & Hu, J. (2023). Adaptively weighted three-way decision oversampling: A cluster imbalanced-ratio based approach. Applied Intelligence, 53(1), 312–335.
[15] Abd El-Naby, A., Hemdan, E. E.-D., & El-Sayed, A. (2023). An efficient fraud detection framework with credit card imbalanced data in financial services. Multimedia Tools and Applications, 82(3), 4139–4160.
[16] Hashemi, S. K., Mirtaheri, S. L., & Greco, S. (2022). Fraud detection in banking data by machine learning techniques. IEEE Access, 11, 3034–3043.
[17] Alamri, M., & Ykhlef, M. (2024). Hybrid undersampling and oversampling for handling imbalanced credit card data. IEEE Access, 12, 14050–14060.
[18] Lopez-Rojas, E. A., Elmir, A., & Axelsson, S. (2016). PaySim: A financial mobile money simulator for fraud detection. In Proceedings of the 28th European Modeling & Simulation Symposium (EMSS) (pp. 249–255). Larnaca, Cyprus.
[19] García, S., Luengo, J., & Herrera, F. (2015). Data preprocessing in data mining (Vol. 72). Cham, Switzerland: Springer.
[20] Chatfield, C. (1986). Exploratory data analysis. European Journal of Operational Research, 23(1), 5–13.