Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 4 (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

An Ensemble Machine Learning Approach for Enhancing Credit Card Fraud Detection

Sarangam Kodati[*1], Nagarjuna Nallametti[2], K. Veeranjaneyulu[3], Nara Sreekanth[4], B. Madhava Rao[5], Gona Jagadesh[6]

[*1]Associate Professor, Department of Information Technology, CVR College of Engineering, Hyderabad, Telangana, 501510, India.

Email ID: k.sarangam@gmail.com

[2]Assistant Professor, Deparment of CSE(AIML), CVR College of Engineering, Hyderabad, Telangana, 501510, India.

Email ID: sri.nnagarjuna@gmail.com n.nagarjuna@cvr.ac.in

[3]Assistant Professor, Department of Information Technology, Hyderabad, Telangana, 501510, India.

Email ID: kveeru876@gmail.com

[4]Associate Professor, Department of Computer Science and Engineering, BVRIT HYDERABAD College of Engineering for Women, Hyderabad, Telangana, India.

Email ID: nara.sreekanthap@gmail.com

[5]Assistant professor, Department of Computer Science and Engineering, Mahatma Gandhi Institute of Technology, gandipet, Hyd-75.

Email ID: bmadhavarao_cse@mgit.ac.in

[6]School of Engineering, Anurag University, Hyderabad, Telangana - 500088, India.

Email ID: jagadeshgona@anurag.edu.in

Cite this paper as: Sarangam Kodati, Nagarjuna Nallametti, K. Veeranjaneyulu, Nara Sreekanth, B. Madhava Rao, Gona Jagadesh, (2025) An Ensemble Machine Learning Approach for Enhancing Credit Card Fraud Detection. *Journal of Neonatal Surgery*, 14 (4), 32-40.

ABSTRACT

The rapid advancement of electronic commerce technology has significantly increased credit card usage, making it the most widely used payment method, there are also more fraud cases linked to them. Since fraudulent activities can be concealed in a wide range of acceptable behaviors, it's challenging to identify credit card theft. These days, online credit card payment systems usually create a predictive model to differentiate between transactions that are fraudulent and non-fraudulent. There is a substantial research gap in the development of effective real-time fraud detection systems that are able to spot fraudulent transactions. Here, it is important to design and put into use efficient models and algorithms that can handle large amounts of streaming data and provide efficient, accurate fraud detection. More recently, techniques based on machine learning (ML) have been designed in order to identify credit card frauds; however, due to the imbalance distribution of classes in each dataset, their detection scores still require improvement. To address these challenges, this paper presents An ensemble machine learning approach for enhancing credit card fraud detection. Here, the fraud is found using the AdaBoost and Logistic Regression techniques. The accuracy, true positive rate (TPR), and F1-score of the model are used to evaluate and compare its performance.

Keywords: *Transactions, logistic regression (LR), Credit Card, Fraud, machine learning, Detection, and AdaBoost (AB)*

1. INTRODUCTION

Digital finance, including supply chain finance, internet lending, and credit card payments, has appeared in recent years, speeding up the transfer of money across industries and increasing the condition of the financial system. As a result of technical advancements, online electronic transactions have gradually changed offline cash transactions in the commodity trade. This credit card transactions are an important component of digital banking that significantly improves people's lives [1]. However, as fraudsters frequently use technical tools (such as Trojan horses and credential stuffing attacks) to steal money from unauthorized accounts, the risks and hidden dangers of credit card transactions are also increasing quickly [2].

For banks and card issuers, since credit card fraud has become more costly, it is now a serious financial security risk. To stop account abuse, financial organizations attempt to implement several security measures [3]. Improving fraud detection techniques and security modules that aim to stop transaction fraud is crucial since fraudsters' techniques evolve over time, and the more advanced the security solution, the more sophisticated the fraudster's techniques will develop [4].

Credit cards offer a convenient and effective way for people to do online transactions. The risk of credit card fraud and misuse has increased as a result of the rise in credit card usage, both financial institutions and credit cardholders face significant financial losses [5]. The complexity and frequency of credit card theft have increased in recent years, presenting serious problems for consumers, businesses, and financial institutions. While the digital era has brought unprecedented convenience to financial transactions, it has simultaneously facilitated the emergence of increasingly sophisticated fraudulent activities [6].

The wide availability of credit cards for payments has made life easier, but it has also presented a number of issues. Through a number of techniques, including Trojan horses, social traps, and certificate stuffing attacks, fraudsters typically steal cardholders accounts and passwords, resulting in significant financial losses throughout the world. As a result, financial institutions work to identify frauds as soon as possible and with accurately [7]. To minimize the negative affect that fraudulent transactions have on the delivery of services, cost-effectiveness, and business reputation, fraud detection has become essential [8]. In the banking sector, detecting credit card fraud is still very difficult, requiring advanced techniques to effectively detect fraudulent activity while reducing false positives [9].

For monetary systems, the detection of credit card fraud is an essential step in identifying and preventing fraudulent transactions. A detection model is used to look at transactions for any suspicious activity. Typically, the detection model is developed using expert-designed rules or rules generated by prior knowledge of fraudulent activity [10]. The difficulty of identifying fraudulent patterns among millions of benign patterns presents an important challenge to the development of an effective algorithm for detecting credit card fraud. Even creating effective rules for people to follow is impossible with this amount of data [11].

Machine learning techniques have become a game-changer in the quickly changing financial sector, especially in the areas of fraud detection and credit risk assessment. Although machine learning models have outperformed traditional statistical approaches in credit risk profiling and credit scoring, false positives are still a significant concern. Inaccurately reporting legal transactions as fraudulent can damage consumer loyalty and confidence, which in turn threatens the credibility of financial institutions that protect their customers' assets [12].

Businesses may benefit from the use of artificial intelligence (AI) and machine learning in the financial sector, including increased satisfaction with customers, lower operating costs, and increased efficiency. A number of machine learning (ML)-based tools have been developed to identify credit card frauds [13]. The number of credit card frauds are committed online through phishing, scamming, or data breaches to fraudulently gain payment information. For the purpose to address the problem of online credit card fraud, numerous methods have been proposed. However, the main challenge facing existing methods when developing an efficient detection model is the high-class imbalance [14]. For this reason, systems that can ensure the security and integrity of any system used are necessary for processing credit card transactions and identifying credit card fraud.

For achieving this, an ensemble machine learning approach to enhance Credit card fraud Detection is proposed. The following is the work is structured: Section II, discusses the literature survey. An ensemble machine learning Approach for Enhancing credit card fraud detection is shown in section III. Section IV evaluates the result analysis. In section V, the conclusion is presented.

2. LITERATURE SURVEY

X. Zhao, Y. Liu and Q. Zhao et. al., [15] offers Enhanced LightGBM for Highly Imbalanced Data and Its Use in credit card fraud identification. Two new ML techniques are presented in this paper: the oversampling cost-harmonization LightGBM (OS-CHL-LightGBM) and the class balancing cost-harmonization LightGBM (CB-CHL-LightGBM). The new methods use LightGBM in combination with class balancing or oversampling technologies to provide the entire solution to the EID problem. They improve LightGBM's performance in CCF detecting scenarios. The two suggested approaches perform better than LightGBM in a number of important performance parameters, according to experimental results on three CCF datasets. In this case, CB-CHL-LightGBM or OS-CHL-LightGBM could increase the F2-score for the first dataset from 0.77 to 0.83, for the second dataset from 0.77 to 0.86, and for the third dataset from 0.70 to 0.82 when compared to the original LightGBM. Class balancing, oversampling, and cost-harmonization loss added independently to LightGBM could not, however, produce better results.

Assaghir Z., M Taher Y., akki S., Hacid M. -S. Haque R., and Zeineddine H. et. al., [16] explains Examining Imbalanced Classification Techniques Experimentally to Identify frauds. To investigate into the usage of machine learning algorithms for fraud detection and to discover solutions to the imbalance classification problem, the study carried out an extensive experiment. Utilizing a dataset labeled with credit card fraud, we gathered our results and determined their credit problems.

According to this study, imbalanced categorization methods are ineffective, particularly when there is a significant imbalance in the data. According to this study, financial institutions face significant costs due to the numerous false alarms caused by the current approaches. This can lead to a rise in fraud cases and inaccurate detection.

Liu G., Xie Y., Jiang C., Yan C., and Zhou M. et. al., [17] explains credit card fraud is detected with a gated network that extracts transactional behavior based on time aware and attention. To ensure that their past transactional behaviors behavioral purpose and periodicity are represented by the proposed framework, it is suggested to use a time-aware-attention module to gather behavioral data from their subsequent historical transactions with time intervals. More thorough and rational representations are designed to be learned through an interaction module. Experiments are conducted on a public dataset and an important dataset of real-world transactions to demonstrate the way the learnt transactional behavioral representations perform.

Boracchi G., Dal Pozzolo A., Alippi C. Caelen O., and Bontempi G. et. al., [18] describes the use of realistic modeling and a novel learning technique for identifying credit card fraud. With the industrial partner's help, the working environment of FDSs, the formalization of the given fraud-detection problem is an appropriate representation of those that regularly analyze massive amounts of credit card transactions. They also provide examples of the best measures of performance to utilize in order to detect fraud. Second, a new learning approach is created that successfully addresses concept drift, class imbalance and verification latency. Third, the impacts of class imbalance and idea drift are illustrated in the tests using a real-world data stream over 75 million transactions were authorized within an interval of three years.

Li Z., Liu G. and Jiang C. et. al., [19] indicates that the research introduces a novel loss function called full center loss (FCL) to be used in deep representation learning to detect fraud with credit cards. Both feature angles and distances are taken into consideration, enabling appropriate deep representation learning monitoring. Through evaluating other complex loss functions with FCL, to demonstrate our model's detection capabilities, they perform a number of tests on two large credit card transaction data sets, one private and one public. Through thorough experiments, the study shows that FCL performs better than other models, suggesting that it may be a more stable model.

J. Song, C. Jiang, G. Zheng, Liu, L. and W. Luan et. al., [20] explains A New Method for using aggregation techniques and feedback mechanisms to identify credit card Frauds. First, in order to create groups of cardholders with similar transaction behaviors, the authors utilize the cardholders past transaction data. A window-sliding technique, therefore, it is suggested that the transactions in each group be combined. The combined transactions and the cardholder's previous transactions are then used to identify a set of particular behavioral patterns for each cardholder. To identify online fraud, a collection of classifiers is trained for every group based on behavioral features. To prevent concept drift, our study demonstrates the advantages of our approach over others by integrating a feedback mechanism into the detection process to detect fraudulent transactions.

A. Mniai, M. Tarik and K. Jebari et. al., [21] gives A New Approach to Identifying Credit Card Fraud. This paper's contribution is the Framework for fraud detection (FFD) that it proposes. First, the framework utilizes an undersampling strategy to address the issue of uneven data. Only relevant characteristics are then chosen using a feature selection (FS) technique. A support vector data description (SVDD) is then utilized to construct the ML model. The goal of SVDD is to separate regular data points from possible variations or outliers by

determining a tight boundary around them. Polynomial self learning PSO (PSLPSO) is a particular version of the particle swarm optimization (PSO) algorithm, is proposed to enhance its hyperparameters C and σ optimization capabilities. Thus, the system's effectiveness is demonstrated by the results of the experiment on a dataset that contains real credit card transactions.

Zhu H., Zhou M., Xie Y. and Albeshri A. et. al., [22] demonstrates the application of an efficient and self-adapting dandelion algorithm for feature selection in the credit card fraud detection. In order to simplify the structure of DA and reduce its number of parameters, this paper proposes an efficient and self-adapting dandelion algorithm. Only the standard sowing operator is kept; the others are taken destroyed. The core dandelion has a seeding radius strategy that is adaptable. The results demonstrate that, in comparison to its competitive peers, the suggested method performs better on the typical test functions while consuming less time. Furthermore, the results demonstrate that, when it comes to feature selection for credit card fraud detection (CCFD), the proposed algorithm can outperform the state-of-the-art methods in terms of classification and detection performance.

Guangquan C., Tingfei H., and Kuihua H. et. al., [23] explains that to use variational auto encoding to detect CCF. This problem is solved by combining traditional deep learning methods with an oversampling method based on variational automatic coding (VAE). To train the classification network, a significant number of different examples from minority groups in a data set with imbalance are generated using the VAE method. An open dataset of credit card fraud transactions from two days in September 2013 involving European cardholders is used to test the suggested approach. According on experimental results, the VAE method outperforms both traditional deep neural network methods and synthetic minority oversampling strategies.

B. Lebichot, T. Verhelst, Y. -A. Le Borgne, L. He-Guelton, F. Oblé and G. Bontempi et. al., [24] explains techniques for detecting credit card fraud using transfer learning. The industrial partner provided a six-month dataset (more than 200 million e-commerce transactions) that was used as the foundation for the case study, which investigated at how detection models developed for one European country could be transferred to another. 15 transfer learning strategies from simple baselines to complex and novel approaches are specifically described and examined, comparing the precision of different transfer situations in a critical and quantitative manner. We make two contributions: (i) The quantity of labeled samples in the target domain has a considerable impact on the accuracy of various transfer procedures, as they demonstrate, and (ii) To address this issue, based on self-supervised and semi-supervised domain adaption classifiers, we offer an ensemble approach.

Mu D., Huang D., Yang L. and Cai X. et. al., [25] introduces CoDetect: Anomaly Feature Detection Combined With FFD. a new fraud detection system called CoDetect that can detect financial fraud by using both network and feature information. Furthermore, CoDetect can concurrently identify patterns of features linked to financial fraud as well as the fraud activity. Numerous tests on both artificial and real-world data show that effective and efficient the suggested methodology is in preventing financial fraud, particularly money laundering.

3. ENSEMBLE MACHINE LEARNING APPROACH FOR ENHANCING CREDIT CARD FRAUD DETECTION

This section presents an Ensemble Machine learning approach to enhance the detection of Credit card fraud. The block diagram of the Ensemble machine learning approach for enhancing Credit card fraud detection is shown in

Figure 1.

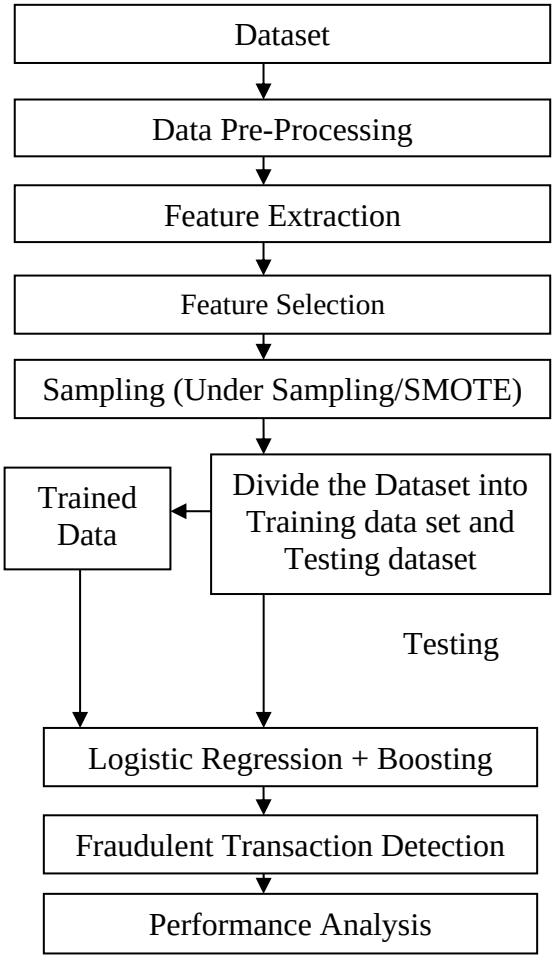

Figure 1: Block Diagram of ensemble Machine Learning Approach for enhancing Credit card Fraud detection

The CCFD dataset used in this analysis is available for download on Kaggle. There are 31 numerical features are included in the dataset. The purpose of the PCA transformation is to protect the data's confidentiality because some of the input variables contain financial information. None of the three provided features were changed. The time between the dataset's

initial transaction and each subsequent transaction is displayed through the "Time" feature. The feature "Amount" shows the amount that was spent on credit card transactions. There are only two possible choices for the label "Class" feature: 0 ordinarily and 1 in the event of a fraudulent transaction.

Pre-processing consists of the following three crucial and typical steps: data formatting is the process of arranging information so that it can be used. The data files should be formatted to be consistent with the rules. CSV files are the most recommended format. cleansing: Since it makes up the majority of the effort, in the data science process, data cleansing is one of the most crucial processes. It involves removing missing information, making naming categories simpler. Sampling is the process of examining subsets from entire, large datasets in order to enhance results and better understand the data's behavior and patterns.

The process of examining the patterns and behavior of the data analysis and selecting the features for additional training and testing is known as feature selection. SMOTE and under-sampling are the two sampling strategies that are utilized. There were two steps in the sample process, which are as follows: Select data entries according to labels (in this case, legitimate or fraudulent). Apply the necessary sampling method to certain data.

To create a single dataset, concatenate all of the data. By choosing a random sample from the primary class, under-sampling is achieved, it is a valid transaction in this case. (designated as 0). By choosing a sample equal to minority class entries and combining data from both classes, the minority class calculated the necessary ratio of random samples, for better model training, the entries for the two classes were made equal in this study.

To properly increase the amount of minority class instances in a dataset, a statistical method known as the synthetic minority over-sampling technique (SMOTE) is used. Using pre-existing minority cases as input, the component generated new instances. To train models as efficiently as feasible, the fraud class (marked as 1) was oversampled for SMOTE in order to have identical entries for each class, making it equivalent to the legitimate class. Additionally, both classes are combined to create a single dataset, similar to under-sampling.

The test data set and the training data set are the two parts of the dataset. Thirty percent of the data set is being tested, and seventy percent is being trained. Test data: The testing procedure begins after the dataset has been used for training. Lastly, the Classifier algorithm is used to train the models. Datasets with labels are collected. The models will be evaluated using the remaining labelled data. Pre-processed data classification requires the application of specific machine learning techniques. Adaboost and logistic regression are the selected classifiers. When it comes to categorization tasks, these algorithms are widely used.

There are similarities between the logistic regression algorithm and the linear regression algorithm. However, logistic regression is used for classification tasks, while linear regression is utilized to predict or forecast results. For both binary and multivariate classification tasks, this approach is simple. There are only two sorts of binomials: 0 and 1. Ordinal is arranged in categories (i.e., very poor, poor, good, very good), but multinomials are of three or more different types and are not ordered.

The machine learning method known as AdaBoost (AB) was primarily created for binary classification. For every instance in the training dataset, the starting weight is assigned to train the AdaBoost algorithm: where the ith training instance is represented by xi and the number of training examples by n, weight (xi) = (1/n). Whether a transaction is fraudulent (1) or not (0) is determined by these two classifiers. Numerous metrics exist for different algorithms, and these metrics were created to evaluate the efficiency of the model. To evaluate the accuracy of different approaches, the terms False Positive (FP), True Negative (TN), False Negative (FN), and True Positive (TP) are commonly used, along with the connection between them. The F1-score, accuracy, and true positive rate (TPR) are used to assess the performance of this model.

TPR is expressed as

$$TPR = \frac{TP}{TP+FN} \quad (1)$$

Accuracy is expressed as

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (2)$$

The F1-score is expressed as

$$F1 - score = \frac{2\times Precision\times Recall}{Precision+Recall} \quad (3)$$

This model achieves better performance for CCFD.

4. RESULT ANALYSIS

This section provides the results of an ensemble ML technique to improving credit card fraud detection. The performance comparison is explained in Table 1.

Table 1: Performance Metrics

Metrics/Methods	Naïve Bayes (NB)	LR+AB
Accuracy (%)	89	95
True Positive Rate (TPR) (%)	88	96
F1-score (%)	87	94

Compared to Naïve Bayes model, Presented Logistic regression and AdaBoost (AB) model has obtained better performance. The Figure 2 describes the TPR comparative Graph.

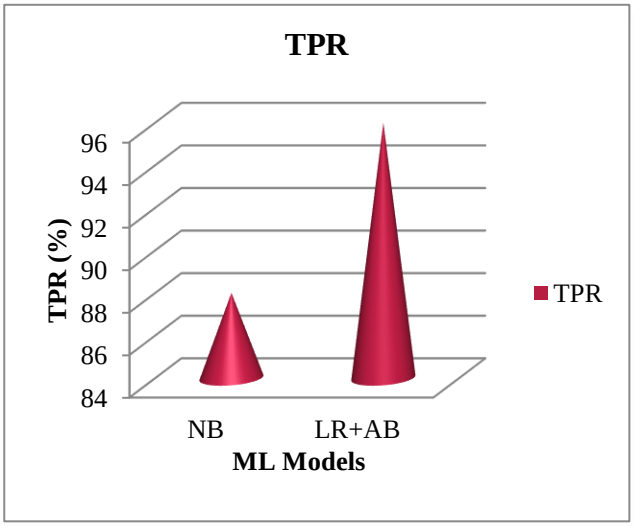

Figure 2: TPR Comparative Graph

The x-axis in figure 2 represents the ML models and y-axis represents the performance (%). The presented model (LR+AB) model has achieved better performance. The Figure 3 presents the Accuracy comparison.

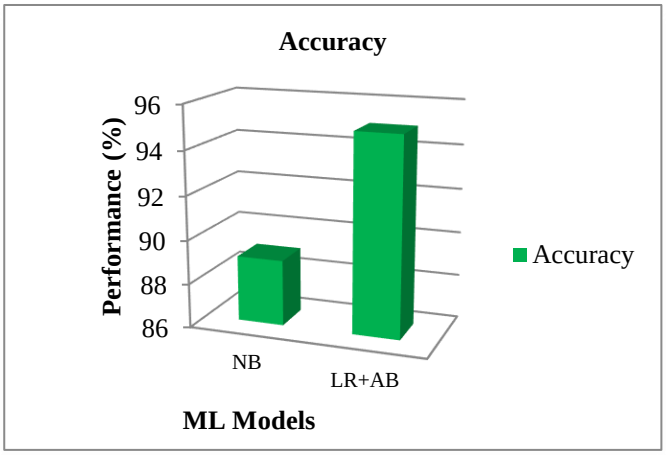

Figure 3: Accuracy Comparison

Figure 3 shows the ML model on the x-axis and the accuracy performance on the y-axis. Compared to previous model, presented model has exhibited high accuracy for CCFD. The Fig 4 describes the f1-score comparison.

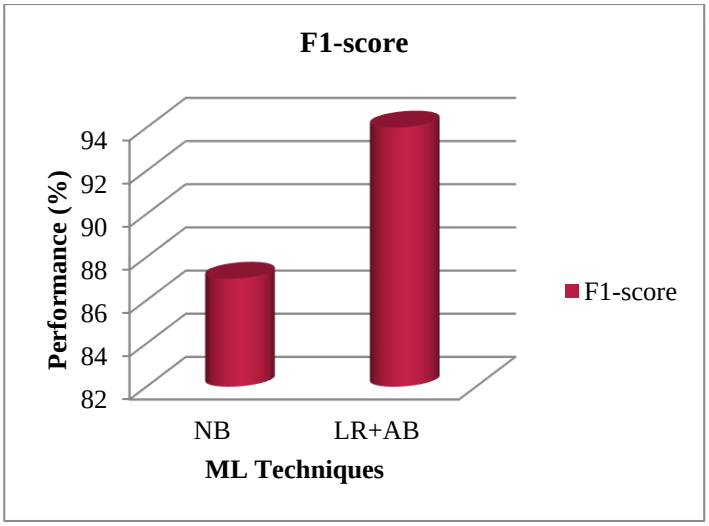

Figure 4: F1-score Comparative Graph

The x-axis in figure 4 represents the ML models and y-axis represents the F1-score performance (%). The Presented model has obtained better f1-score than other models. From the results, it has been noted that this approach has outperformed others in identifying credit card fraud. This approach can therefore be applied in real time to the detection of fraud in a number of sectors.

5. CONCLUSION

An issue that frequently causes banks and credit card companies to lose money, and individuals equally is credit card fraud. This analysis presents an ensemble machine learning approach to improve the detection of credit card fraud. After gathering and preprocessing the Kaggle credit card dataset, the issues with unbalanced data are addressed by the SMOTE model. The model's accuracy is enhanced by classifying the data into training and testing groups and choosing appropriate features. These trained and testing data is applied to ML model i.e. Logistic Regression and AdaBoost algorithms. The LR+AB model detects and classifies the transaction data as Fraud or not. Whenever it came to detecting credit card fraud, the model performed better than previous models, according to evaluations of its TPR, F1-score, and accuracy. The fraud detection model's performance has been greatly enhanced by this model. This technique will be applied in real time to detect fraud in the financial and banking industries.

REFERENCES

[1] N. Ferdous Aurna, M. Delwar Hossain, L. Khan, Y. Taenaka and Y. Kadobayashi, "FedFusion: Adaptive Model Fusion for Addressing Feature Discrepancies in Federated Credit Card Fraud Detection," in *IEEE Access*, vol. 12, pp. 136962-136978, 2024, doi: 10.1109/ACCESS.2024.3464333.

[2] K. Zhu, N. Zhang, W. Ding and C. Jiang, "An Adaptive Heterogeneous Credit Card Fraud Detection Model Based on Deep Reinforcement Training Subset Selection," in *IEEE Transactions on Artificial Intelligence*, vol. 5, no. 8, pp. 4026-4041, Aug. 2024, doi: 10.1109/TAI.2024.3359568.

[3] H. Zhu, M. Zhou, G. Liu, Y. Xie, S. Liu and C. Guo, "NUS: Noisy-Sample-Removed Undersampling Scheme for Imbalanced Classification and Application to Credit Card Fraud Detection," in *IEEE Transactions on Computational Social Systems*, vol. 11, no. 2, pp. 1793-1804, April 2024, doi: 10.1109/TCSS.2023.3243925.

[4] L. Ni, J. Li, H. Xu, X. Wang and J. Zhang, "Fraud Feature Boosting Mechanism and Spiral Oversampling Balancing Technique for Credit Card Fraud Detection," in *IEEE Transactions on Computational Social Systems*, vol. 11, no. 2, pp. 1615-1630, April 2024, doi: 10.1109/TCSS.2023.3242149.

[5] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan and M. Ahmed, "Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms," in *IEEE Access*, vol. 10, pp. 39700-39715, 2022, doi: 10.1109/ACCESS.2022.3166891.

[6] E. Ileberi and Y. Sun, "Advancing Model Performance With ADASYN and Recurrent Feature Elimination and Cross-Validation in Machine Learning-Assisted Credit Card Fraud Detection: A Comparative Analysis,"

in *IEEE Access*, vol. 12, pp. 133315-133327, 2024, doi: 10.1109/ACCESS.2024.3457922.

[7] Y. Xie *et al.*, "A Spatial–Temporal Gated Network for Credit Card Fraud Detection by Learning Transactional Representations," in *IEEE Transactions on Automation Science and Engineering*, vol. 21, no. 4, pp. 6978-6991, Oct. 2024, doi: 10.1109/TASE.2023.3335145.

[8] P. Kalpana, S. Kodati, N. Sreekanth, H. M. Ali, and R. A C, 'Predictive Analytics for Crime Prevention in Smart Cities Using Machine Learning', in *2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS)*, 2024, pp. 1–4. https://doi.org/10.1109/IACIS61494.2024.10721948..

[9] D. Lunghi, G. M. Paldino, O. Caelen and G. Bontempi, "An Adversary Model of Fraudsters' Behavior to Improve Oversampling in Credit Card Fraud Detection," in *IEEE Access*, vol. 11, pp. 136666-136679, 2023, doi: 10.1109/ACCESS.2023.3337635.

[10] T. -T. -H. Le, Y. Hwang, H. Kang and H. Kim, "Robust Credit Card Fraud Detection Based on Efficient Kolmogorov-Arnold Network Models," in *IEEE Access*, vol. 12, pp. 157006-157020, 2024, doi: 10.1109/ACCESS.2024.3485200.

[11] Kalpana, P. K. Malleboina, M. Nikhitha, P. Saikiran and S. N. Kumar, "Predicting Cyberbullying on Social Media in the Big Data Era Using Machine Learning Algorithm," *2024 International Conference on Data Science and Network Security (ICDSNS)*, Tiptur, India, 2024, pp. 1-7, https://doi.org/10.1109/ICDSNS62112.2024.10691297..

[12] M. Adil, Z. Yinjun, M. M. Jamjoom and Z. Ullah, "OptDevNet: A Optimized Deep Event-Based Network Framework for Credit Card Fraud Detection," in *IEEE Access*, vol. 12, pp. 132421-132433, 2024, doi: 10.1109/ACCESS.2024.3458944.

[13] P. Kalpana, P. Srilatha, G. S. Krishna, A. Alkhayyat and D. Mazumder, "Denial of Service (DoS) Attack Detection Using Feed Forward Neural Network in Cloud Environment," *2024 International Conference on Data Science and Network Security (ICDSNS)*, Tiptur, India, 2024, pp. 1-4, https://doi.org/10.1109/ICDSNS62112.2024.10691181..

[14] F. A. Ghaleb, F. Saeed, M. Al-Sarem, S. N. Qasem and T. Al-Hadhrami, "Ensemble Synthesized Minority Oversampling-Based Generative Adversarial Networks and Random Forest Algorithm for Credit Card Fraud Detection," in *IEEE Access*, vol. 11, pp. 89694-89710, 2023, doi: 10.1109/ACCESS.2023.3306621.

[15] X. Zhao, Y. Liu and Q. Zhao, "Improved LightGBM for Extremely Imbalanced Data and Application to Credit Card Fraud Detection," in *IEEE Access*, vol. 12, pp. 159316-159335, 2024, doi: 10.1109/ACCESS.2024.3487212.

[16] S. Makki, Z. Assaghir, Y. Taher, R. Haque, M. -S. Hacid and H. Zeineddine, "An Experimental Study With Imbalanced Classification Approaches for Credit Card Fraud Detection," in *IEEE Access*, vol. 7, pp. 93010-93022, 2019, doi: 10.1109/ACCESS.2019.2927266.

[17] Y. Xie, G. Liu, C. Yan, C. Jiang and M. Zhou, "Time-Aware Attention-Based Gated Network for Credit Card Fraud Detection by Extracting Transactional Behaviors," in *IEEE Transactions on Computational Social Systems*, vol. 10, no. 3, pp. 1004-1016, June 2023, doi: 10.1109/TCSS.2022.3158318.

[18] A. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi and G. Bontempi, "Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy," in *IEEE Transactions on Neural Networks and Learning Systems*, vol. 29, no. 8, pp. 3784-3797, Aug. 2018, doi: 10.1109/TNNLS.2017.2736643.

[19] Z. Li, G. Liu and C. Jiang, "Deep Representation Learning With Full Center Loss for Credit Card Fraud Detection," in *IEEE Transactions on Computational Social Systems*, vol. 7, no. 2, pp. 569-579, April 2020, doi: 10.1109/TCSS.2020.2970805.

[20] C. Jiang, J. Song, G. Liu, L. Zheng and W. Luan, "Credit Card Fraud Detection: A Novel Approach Using Aggregation Strategy and Feedback Mechanism," in *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3637-3647, Oct. 2018, doi: 10.1109/JIOT.2018.2816007.

[21] A. Mniai, M. Tarik and K. Jebari, "A Novel Framework for Credit Card Fraud Detection," in *IEEE Access*, vol. 11, pp. 112776-112786, 2023, doi: 10.1109/ACCESS.2023.3323842.

[22] H. Zhu, M. Zhou, Y. Xie and A. Albeshri, "A Self-Adapting and Efficient Dandelion Algorithm and Its Application to Feature Selection for Credit Card Fraud Detection," in *IEEE/CAA Journal of Automatica*

Sinica, vol. 11, no. 2, pp. 377-390, February 2024, doi: 10.1109/JAS.2023.124008.

[23] H. Tingfei, C. Guangquan and H. Kuihua, "Using Variational Auto Encoding in Credit Card Fraud Detection," in *IEEE Access*, vol. 8, pp. 149841-149853, 2020, doi: 10.1109/ACCESS.2020.3015600.

[24] B. Lebichot, T. Verhelst, Y. -A. Le Borgne, L. He-Guelton, F. Oblé and G. Bontempi, "Transfer Learning Strategies for Credit Card Fraud Detection," in *IEEE Access*, vol. 9, pp. 114754-114766, 2021, doi: 10.1109/ACCESS.2021.3104472.

[25] D. Huang, D. Mu, L. Yang and X. Cai, "CoDetect: Financial Fraud Detection With Anomaly Feature Detection," in *IEEE Access*, vol. 6, pp. 19161-19174, 2018, doi: 10.1109/ACCESS.2018.2816564.