InternationalJournalonRecentandInnovationTrendsinComputingand Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
ArticleReceived:*11 August2023****Revised:****28September2023* ***Accepted:****19 October2023*

EnsembleLearningforfrauddetectioninOnline Payment System

FraudDetectioninOnlinePaymentSystem

Kothapalli.Mandakini[1],
[1]Research Scholar, Department of CSE, Hyderabad. Mail Id:kothapallymandakini@gmail.com

Abstract: - The imbalanced problem in fraud detection systems refers to the unequal distribution of fraud cases and non-fraud cases in the information that is used to train machine learning models. This can make it difficult to accurately detect fraudulent activity. As a general rule, instances of fraud occur much less frequently than instances of other types of occurrences, which results in a dataset which is very unbalanced. Thisimbalancecanpresentchallengesformachinelearningalgorithms,astheymaybecome biasedtowardsthemajorityclass(thatis,non-fraud cases) and fail to accuratelydetect fraud. In situations like these, machine learning models mayhavea highaccuracy overall,buta low recall for the minority class (i.e., fraud cases), which means that many instances of fraud will be misclassified as instances of something else and will not be found. In this study, Synthetic Minority SamplingTechnique (SMOTE) is used for balancing the data set and the following machine learning algorithms such as decision trees, Enhanced logistic regression, Naive Bayes are used to classify the dataset.MajorityVoting mechanism is used to ensemble the DT,NB, ELR methods and analyze the performance of the model. The performance of the Ensemble of various Machine Learning algorithms was superior to that of the other algorithms in terms of accuracy (99.62%), F1 score (95.21%), precision(98.02%), and recall (96.75%).

Keywords: Ensemble Learning, Extreme Imbalanced dataset, Fraud Detection, Machine Learning, Majority voting, Online Payment System, SMOTE etc.

I.INTRODUCTION:

In the context of credit and debit card fraud detection, the term "imbalanced data" refers to a problem that is common in machine learning and occurs when the number of examples of fraudulent transactions is significantly lower than thenumberof examplesof legitimate transactions.This can result in a biased model that has a higher probability of classifying all transactions as legitimate, which leads to a highrateoffalsenegativesandalossofvisibilityintoactual instances of fraud. To address this issue, various techniques can be used to balance the data, such as:

Increasing the sample size of the less common class (fraudulent transactions) either by duplicating existing cases orcreatingentirelynewexamplesinordertoachieveamore even distribution.

Undersampling the predominant class (legal transactions) through the use of a random selection process in order to achieve a more equitable distribution.

Sometimes referred to simply as "SMOTE," the Synthetic MinorityOver-SamplingTechnique(SMOTE)creates synthetic examples of the minority class by extrapolating between real-world examples.

To train the model to prioritise fraud detection, cost-sensitive learning adjusts the learning algorithm to account for the consequences of both false negatives and false positives.

The accuracy of the model used to detect fraud can be improved with the help of these strategies, as can the elimination of bias to the mainstream class. Nevertheless, it isessentialto determine howthe method of choice willhave aneffectonthemodel'sefficiencyasawhole andtopickthe approach that will provide the most degree of success in meeting the requirements of the application.

Identifying and preventing fraudulent credit cardtransactions is a crucial task in the financial sector. Banks andotherfinancialinstitutionsfaceaseriouschallengewhen dealing with fraudulent transactions due to the potential for both financial and reputational harm. The patterns and characteristics of credit card transactions are often analysed by machine learning algorithms in order to spot fraudulent activity.

However, the information that is utilised to train algorithms is frequently highly unbalanced, with a significantly higher percentage of cases that do not involve fraud compared to cases that do involve fraud. This imbalance can pose significant challenges for ML algorithms, as they might become biased to the majority class and fail to accurately detect fraud. In such cases, machine learning models may have a high overall accuracy but a low recall for theminority class, meaning that many fraud cases may be misclassified as non-fraud and not detected.

Techniques range from oversampling the minority group to under sampling the majority group to stratified sampling or employing cost-sensitive learning, are all potential solutions to the imbalance issue that arises in the process of detecting fraudulent credit card activity.Additionally, it is essential to make use of relevant performance indicators, such as F1-score, Recall & precision which take into consideration the imbalance in the data and appropriately demonstrate how well the anti-fraud measures are working.

Theproblemofimbalanceiscomplicated,withmanyfactors involved. challenges exist in detecting credit card fraud,such as the infrequent occurrence of fraud and the difficulty in collecting a representative sample of fraud cases. To overcome these challenges, it is important to employ a combination of data pre-processing techniques, such as feature selection and normalization, as well as advanced machine-learning models, such as deep-learning and ensemble methods, to achieve a high-performing fraud detection system.

In conclusion, the imbalance problem in credit card fraud identification or detection is a complicated and hard subject that calls for a methodology that takes into account multiple dimensions.Itispossibletoachieveahigh-performingfraud detection system by overcoming the imbalance problem and combining appropriate techniques for balancing the data, using appropriate performance metrics, and employing advanced models of Machine learning. This will let for the system to be more accurate.

II.REVIEWOF RELEVENT WORK

The papers [1,3,7] discuss about the problem of unbalanced data in detecting credit card fraud and how it affects how well machine learning algorithms work. The method of random under-sampling, as well as the synthetic minority over-sampling technique, is one of the resampling strategies that are suggested in the paper [1] to balance the data. The paper reports that random under-sampling achieved a better F1-score compared to SMOTE, with a F1-score of 0.99 and 0.94, respectively.

The paper [2] introduces a new method called MixBoost for handling imbalanced data. MixBoost is a synthetic oversampling technique that uses the idea of mixup to generatesyntheticsamples.ThepaperreportsthatMixBoost achieved a greater F1-score equated to other oversampling methods such as SMOTE, with a F1-score of 0.97.

The paper [3] discusses several methods for dealing with skewed data in the context of credit card fraud detection, such as resampling strategies, ensemble methods and cost-sensitive learning,According to the findings of the research paper, the method under consideration, which is a hybrid of resampling strategies and cost-sensitive learning, attained a score of 0.97 on the F1-scale.

In the research paper [4], the authors evaluate and contrast the effectiveness of a number of different machine learning algorithms, such as support vector machines, decision trees, and random forests, when applied to imbalanced classes. In comparison to the other algorithms, the random forest algorithm was found to have the highest F1 scoreof0.98, as stated in the paper.

In the research paper [5,] the authors propose a novelmethod for detecting click fraud from highly skewed user click data. This method is referred to as the Quad-Division- Prototype-Selection based k-Nearest Neighbor (QDPS- KNN) classifier. According to the findings of the study, the F1-score achieved by QDPS-KNN was 0.94, which was significantly higher than the F1-scores achieved by other traditional classification algorithms.

Theresearchpaper[6]presentsalogisticregressionlearning model as a solution to the problem of handling concept drift in credit card fraud detection systems when dealing with unbalanced data.According to the findings of the paper, the approach that wasproposedmanaged toachieve an F1 score of 0.97.

The papers [8, 9, and 10] discuss the various methods that can be used to identify fraudulent activity involving credit cards. In the article [8], the authors propose an approach to evolutionary multi-label classification that is based on soft computing.According to the findings, the proposed method performed significantly better than any of the other multi-label classification approaches in terms of precision, recall, F1-score, and accuracy. By bagging multiple boosted trees, the authors of [9] suggested a hybrid multi-level system for detecting credit card fraud. Comparing the proposed system to more conventional machine learning methods, the results demonstrated an improvement in accuracy and precision for fraud detection.

By combining balancing methods and an ensemble strategy, the authors of [10] were able to successfully detect credit card fraud. The outcomes demonstrated that, in comparison to conventional machine learning methods, the proposed method enhanced accuracy and decreased false positives.

Oversampling and feature selection methods for fraud detection are the focus of papers [11] and [13]. Multiple correspondence analysis based on an importance factor is proposedformultimediadatain[11].Incomparisontomore conventional approaches, the results demonstrated that the proposed method resulted in more precise analysis of multimedia data.

In [13], the authors compose AI-based feature selection strategies and oversampling strategies for detecting banking fraud.Theoutcomesdemonstrated thattheproposedmethod outperformed more conventional machine learning approaches when it came to detecting fraud.

An unbalanced dataset in the financial services industry is the focus of paper [12]. For mining skewed data sets, the authors propose a new hybrid under sampling approach. When compared to standard oversampling methods, the outcomes demonstrated that the proposed approach significantlyenhancedtheprecisionofimbalanceddatasets.
[14] Using a stacked ensemble of models trained with heterogeneous bagging, the paper's authors propose a new approach to dealing with class imbalance in the detection of creditcardfraud.Theycomparetheirmethodtothestate-of- the-art approaches anddemonstrate its superiorperformance on several datasets.

In [15], the author provides a wide-ranging analysis of unbalanced-learning approaches to financial insolvency forecasting. The paper covers various methods including oversampling, under sampling, cost-sensitive learning, ensemble methods, and deep learning methods. The author provides a detailed comparison of these methods and concludes that ensemble methods are the most effective for dealing with imbalanced data.

[16] In this paper, we propose a hybrid approach that brings together dynamic weighted entropy and conventional imbalanced learning strategies. Experiments conducted on a fraudulent credit card transactions dataset reveal that the method achieves higher accuracy rates than the state-of-the-art approaches.

[17]Inthispaper,theauthorsexaminehowclassdifferences affect the development of false positives when detecting credit card fraud. The authors propose an ensemble-based approach to solving the issue and assess the method's efficacyonseveraldatasets.Theoutcomesdemonstratethat their strategy effectively deals with class disparity and concept shift.

To address the issue of extreme class imbalance when detecting credit cardfraud, the authors of paper [18] analyse and compare several algorithms that operate on the data level. They test the effectiveness of these techniques on various datasets and demonstrate that oversampling and price-sensitive learning techniques deliver the best results.

To address class imbalance issues in commercial settings,the authors of [19] propose a budget-friendly ensemble of stacked denoising autoencoders. Several datasets are used to demonstrate the method'ssuperior performance compared to the state-of-the-art.

In conclusion, the studies highlight the significance of handling unbalanced data and the effect it has on the effectiveness of machine learning models in the detection of credit card fraud. There are a few different approaches that have been suggested for dealing with imbalanced data.These approaches include resampling strategies, cost- sensitive learning, and ensemble methods. While F1-scores achieved by the various strategies range widely, all of them demonstrate a strong ability to identify credit card fraud.

III.IMBALANCEDATAHANDLING USING MACHINE LEARNING

One of the most important and hard problems to solve in machine learning and data analysis is how to deal with imbalanced data when detecting fraud. The fact that the minority class, which in this context refers to the instancesoffraudulentactivity,isunderrepresentedisthefundam ental problem that develops as a consequence of the imbalanced data. Because of this, the model is skewed in favour of the class that constitutes the majority. When it comes to the process of detecting instances of fraud, this results in poor performanceandalowlevelofaccuracy.Whendealingwith skewed data, the discipline of fraud detection finds success with three machine learning algorithms: decision trees,linear regression, and Naive Bayes.

Decision Trees are tree-based models that use a recursive approach to split the data into smaller subsets. They can be used to identify the important features that contribute to fraud. DecisionTrees are a good choice for imbalanced data as they can handle missing values, non-linear relationships, and multi-class classification problems. However, decision trees can also overfit to the data and may not perform wellon unseen data.

Linearregressionisawaytomodeltherelationshipbetween variables that are independent and variables that are dependent.Astheoutputiseasilyconvertedtoabinary

value, it can be put to use in binary classification problems like fraud detection. Linear Regression is sensitive tooutliers and may not perform well in the presence of non- linear relationships.

Naive Bayes is a probabilistic algorithm that assumes independence between features. It calculates the probability of a class given a set of features. Naive Bayes can handle imbalanced data by adjusting the class prior probabilities to account for the imbalance. However, it may not performwell on data with complex relationships between features.

The term "data wrangling," also known as "data munging," refers to the procedure of preparing unstructured data for further study.There are a lot of entries and characteristics in this data set, as evidenced by the enormous number of rows and columns (284807). When one group of data is much bigger than the other, this is known as imbalanced data. Issues arise when attempting to model and train machine learning algorithms when this occurs. Oversampling, under sampling,andthecreationofsyntheticdataareonlysomeof the methods that can be employed to deal with skewed information. The characteristics of the data, as well as the objectives of the analysis, will guide the selection of the appropriate method.

The introduction of duplicate values into a dataset can leadto inaccuracies and biases in the analysis; as a result, it is essential that these values be located and removed. This can be done through various methods such as checking for duplicates based on unique identifier(s) in the dataset, using Pandas duplicated() function or by comparing the data manually. After identifying the duplicated values, they can be dropped from the dataset using methods such as the Pandas drop_duplicates() function or by filtering the data in a new DataFrame without the duplicates. It is important to note that while removing duplicates can help improve the accuracy of analysis, it is necessary to also consider other data cleaning techniques such as handling missing values, fixing inaccuracies, and handling outliers to advance the overall superiority of the data.

In the field of machine learning, SMOTE is a well-known method for data balancing. Creating artificial samples of the underrepresented group enables this technique to rectify imbalances in datasets. The algorithm operates by first selecting a sample from a minority class, then locating the k samples that are geographically closest to it, and finally generating new samples by interpolating the characteristics of the marginal class sample and its neighbours. By developing synthetic samples that are not perfect replicas of the original minority class samples, this strategy helps to addresstherestrictionsthatcanbecausedbyoversampling, which can lead to over fitting. SMOTE is a strategy that has been widely embraced by the community of machine learning due to its robustness and efficiency in dealing with imbalanced data in the context of fraud detection.

In conclusion, Decision Trees, Linear Regression, Logistic RegressionandNaiveBayesarefourmethodologiesthatcan be utilised in the process of fraud detection to deal with imbalanced data. Each approach has certain advantages as well as drawbacks; the method that is ultimately selectedwill be determined by the particular parameters of the issue at hand.

IV.RESULTSANDDISCUSSION

A type of algorithm for machine learning known as a Decision Tree generates predictions by employing a model that resembles a tree. On the basis of the characteristics or variables contained within the data, the algorithm employs a recursive partitioning process in order to divide the information into ever-more specific subgroups of data. In order to achieve the greatest possible degree of accuracy in the categorization of the data, the purpose of this techniqueis to locate the division points that will yield the bestpossible results. In the framework of the investigation of fraudulent use of credit cards, a Decision Tree could be utilised to partition the data into various sub-groups according to the properties of the transactions, such as the amount, the location, the time of day, and so on. For example, the Decision Tree could divide the data into sub- groups based on the characteristics of the transactions.

The resultsobtained from Decision Tree Model as: - Accura cy: 0.9462, recall_Score: 0.9262, Precision_score: 0.965, F1 -score equals: 0.9452. The confusion matrix of the same is a s shown in the figure 1.

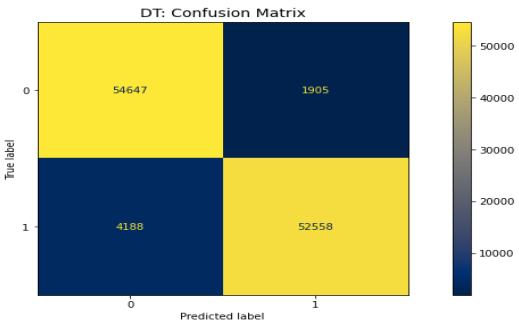

Figure1.ConfusionMatrixforDecisionTree

When applied to the test dataset, a Decision Tree with an accuracy of 94.62% was able to correctly predict 94.62% of the cases. However, it is important to keep in mind that accuracy isnotalwaysthe bestperformance metricfor fraud detectionbecauseitcanbemisleadingwhenthereisan

InternationalJournalonRecentandInnovationTrendsinComputingand Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
ArticleReceived:11 August2023Revised:28September2023 Accepted:19 October2023

unbalanced dataset present. This accuracy value demonstrates that the algorithm is doing a good job with the data. Other metrics, such as F1 Score, precision and recall, that accurately reflect the effectiveness of the frauddetection system, are frequently more appropriate. These metrics take into account the imbalance in the data.

Logistic Regression is a technique that is frequently utilised for classification problems, including the detection of credit card fraud. The algorithm uses a logistic function to model the relationship between the features or variables in the data andtheprobabilityofatransactionbeingfraudornon-fraud. The algorithm then uses this model to make predictions about new transactions.

The Enhanced Logistic Regression (ELR) model considers the independent features and maps these features with the batch feature set and the multi-level independent

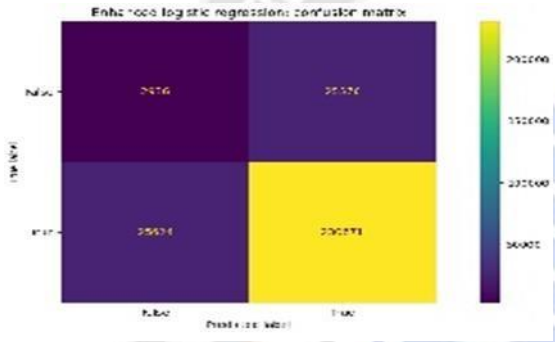

Figure2.ConfusionMatrixforEnhancedLogistic Regression

Feature set is generated and it takes it this set of features as input to detect the fraud transactions from legitimate ones.

ELR Model has scores as:- Accuracy: 0.9544, recall_Score: 0.9139,Precision_score:0.9729,F1-scoreequals:0.9425. Fi gure2depictstheconfusionmatrixusedin EnhancedLogist ic Regression (ELR).
The fact that Enhanced Logistic Regression achieved an accuracyof95.44%indicatesthatthealgorithmsuccessfully predicted 95.44% of the cases contained in the test dataset. This accuracy value, similar to that of the Decision Tree, indicates that the algorithm is performing well; however, Itis essential to take into consideration alternativeperformance metrics in order to make up for the disparity in the data.

Bayes' theorem, which may be thought of as a probabilistic method of making predictions, serves as the foundation for the Naive Bayes algorithm. Given the characteristics or variables that are contained in the data, the Naive Bayes methodgeneratesestimatesbasedontheprobabilities associated with each class.The premise that the attributes or variables are not reliant on one another is what gives this algorithm its name, "Naive," and it's also the meaningbehind its nickname.

The fact that the Naive Bayes algorithm achieved aprecision of 91.05% indicates that it acceptably forecast 91.05% of the cases contained in the test dataset. This accuracy value, like the accuracy values for the other algorithms, indicates that the algorithm is performing well; however, it is significant to consider other performance metrics that account for the imbalance in the data.

Table1ComparisonofdifferentModels

Model	Model Accuracy	Model F1-Score	precision	recall
Decision Tree	94.62%	94.62 %	96.50%	92.62%
Enhanced Logistic regression	95.44%	94.41 %	97.29%	91.39%
Naïve Bayes	91.05%	91.01 %	97.02%	84.73%
Ensemble of DT,NB,ELR	99.62%	95.21 %	98.02%	96.75%

Ensemble of DT,NB, ELR had shown the greatest accuracy than other models. The performance metrics are Accuracy:- 99.62%,F1-Score:-95.21%,Precision:- 98.02%,Recall:- 96.75%.

Enhanced Logistic Regression had a similar level of performancewithaModelAccuracyof95.44%andaModel F1-Score of 94.41%. Its precision was even higher, at 97.29%. However, its recall was lower than DecisionTree's, at 91.39%.

Decision Tree (DT) was shown the next greatest accuracy rate when compared to the other two machine learning models we looked at (Enhanced Logistic Regression and Naive Bayes). DT coming in at 94.62% accurate. This is reflected not only in its Model F1-Score but also in its precision, which comes in at 94.62% and 96.50% respectively. The memory of Decision Tree was 92.62% accurate.

Naive Bayes had the lowest accuracy rate among the three models, at 91.05%. Its Model F1-Score and precision were also lower, at 91.01% and 97.02% respectively. Its recallwas 84.73%.

Overall, Ensemble of DT,NB,ELR outperformed than other models in terms of precision, F1-score, accuracy, and recall.

V.CONCLUSION

In order to identify fraudulent behaviour, many popular machine learning techniques are used. These include the Decision Tree, Enhanced Logistic Regression, and Naive Bayes. The effectiveness of these algorithms in determining whether or not a transaction is fraudulent has been analysed and rated. According to the findings, Ensemble of DT,NB,ELR has the highest accuracy, coming in at 99.62%. This is followed by Enhanced Logistic Regression, which has an accuracy of 95.44%,and DecisionTree,which has an accuracy of 94.62%. However, when selecting an algorithm for fraud detection, it is essential to take into account other aspects, such as the amount of computational resources it requires, how easily it can be interpreted, and how easily it can be scaled. In general, each of these algorithms has its own set of benefits and drawbacks, and the decision regarding which one to use depends on the particular demands of the activity that is currently being performed.

REFERANCES

[1] P.Parekh,C.Rana,K.Nalawade,andS.Dholay,"CREDIT CARDFRAUDDETECTIONWITHRESAMPLING TECHNIQUES," in 2021 12th InternationalConference on ComputingCommunicationandNetworkingTechnologies, ICCCNT 2021, 2021, doi: 10.1109/ICCCNT51525.2021.9579915.

[2] A. Kabra et al., "MixBoost: Synthetic oversampling using boosted mixup for handling extreme imbalance," in Proceedings - IEEE International Conference on Data Mining, ICDM, 2020, vol. 2020-November, doi: 10.1109/ICDM50108.2020.00129.

[3] I.A.Mondal,M.E.Haque,A. M.Hassan, and S. Shatabda, "Handling Imbalanced Data for Credit Card Fraud Detection," in 24th International Conference on Computer and Information Technology, ICCIT 2021, 2021, doi: 10.1109/ICCIT54785.2021.9689866.

[4] S. Datta and A. Arputharaj, "An Analysis of Several Machine Learning Algorithms for Imbalanced Classes," in 5th International Conference on Soft Computing and Machine Intelligence, ISCMI 2018, 2018, doi: 10.1109/ISCMI.2018.8703244.

[5] D. Sisodia and D. S. Sisodia, "Quad division prototype selection-based k-nearest neighbor classifier for click fraud detection from highly skewed user click dataset," Eng. Sci. Technol. an Int. J., vol. 28, 2022, doi: 10.1016/j.jestch.2021.05.015.

[6] P.KulkarniandR.Ade,"Logisticregressionlearningmodel for handling concept drift with unbalanced data in credit card fraud detection system," Adv. Intell. Syst. Comput., vol. 380, 2016, doi: 10.1007/978-81-322-2523-2_66.

[7] H. Shen and J. Cao, "Imbalanced research of deep belief network based on dynamic cost sensitive," in ACM International Conference Proceeding Series, 2019, doi: 10.1145/3330530.3330539.

[8] R. Aslam, M. I. Tamimy, and W. Aslam, "Soft computing based evolutionary multi-label classification," Intell. Autom. Soft Comput., vol. 26, no. 6, 2020, doi: 10.32604/iasc.2020.013086.

[9] M. Kavitha and M. Suriakala, "Hybrid Multi-Level Credit Card Fraud Detection System by Bagging MultipleBoosted Trees (BMBT)," in 2017 IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2017, 2018, doi: 10.1109/ICCIC.2017.8524161.

[10] S. Taneja, B. Suri, and C. Kothari, "Application of Balancing Techniques with Ensemble Approach for Credit Card Fraud Detection," in 2019 International Conferenceon Computing, Power and Communication Technologies, GUCON 2019, 2019.

[11] Y.Yang,S.Pouyanfar,H. Tian,M.Chen,S.C.Chen,and M. L. Shyu, "IF-MCA: Importance Factor-Based Multiple Correspondence Analysis for Multimedia Data Analytics," IEEE Trans. Multimed., vol. 20, no. 4, 2018, doi: 10.1109/TMM.2017.2760623.

[12] G. G. Sundarkumar and V. Ravi, "A novel hybrid undersampling method for mining unbalanced datasets in banking and insurance," Eng. Appl. Artif. Intell., vol. 37, 2015, doi: 10.1016/j.engappai.2014.09.019.

[13] B. Itri, Y. Mohamed, B. Omar, and Q. Mohamed, "Composition of feature selection methods and oversampling techniques for banking fraud detection with artificial intelligence,"International JournalofEngineering Trends and Technology, vol. 69, no. 11. 2021, doi: 10.14445/22315381/IJETT-V69I11P228.

[14] V. Sobanadevi and G. Ravi, "Handling data imbalance using a heterogeneous bagging-based stacked ensemble (hbse) for credit card fraud detection," in Advances in Intelligent Systems and Computing, 2021, vol. 1167, doi: 10.1007/978-981-15-5285-4_51.

[15] T. Le, "A comprehensive survey of imbalanced learning methods for bankruptcy prediction," IET Communications, vol. 16, no. 5. 2022, doi: 10.1049/cmu2.12268.

[16] Z. Li, M. Huang, G. Liu, and C. Jiang, "Ahybrid method with dynamic weighted entropy for handling the problemof class imbalance with overlap in credit card fraud detection," Expert Syst. Appl., vol. 175, 2021, doi: 10.1016/j.eswa.2021.114750.

[17] S. Priya and R. A. Uthra, "Comprehensive analysis for class imbalance data with concept drift using ensemble based classification,"J.AmbientIntell.Humaniz.Comput., vol. 12, no. 5, 2021, doi: 10.1007/s12652-020-01934-y.

[18] A.Singh,R.K.Ranjan,andA.Tiwari,"CreditCardFraud Detection under Extreme Imbalanced Data:AComparative

Study of Data-level Algorithms," J. Exp. Theor. Artif. Intell., vol. 34, no. 4, 2022, doi: 10.1080/0952813X.2021.1907795.

[19] M. L. Wong, K. Seng, and P. K. Wong, "Cost-sensitive ensemble of stacked denoising autoencoders for class imbalance problems in business domain," Expert Syst. Appl., vol. 141, 2020, doi: 10.1016/j.eswa.2019.112918.