Online payments Fraud Detection using Machine Learning models

T.G.Ramnadh Babu1, Dr. Sireesha Moturi2, Ch.Sandeep3, R.Chaitanya Santosh4, P.Lucky5, Dr. S. Siva Nageswarao6, and Dodda Venkata Reddy7

1Asst.Professor,Department of CSE, Narasaraopeta Engineering College, Narasaraopet, India. 3,4,5Student,Department of CSE, Narasaraopeta Engineering College, Narasaraopet, India. 2,6Assoc.Professor,Department of CSE, Narasaraopeta Engineering College, Narasaraopet, India. baburamnadh@gmail.com

Abstract:

The increasing popularity of e-commerce and reliance on var ious online payment systems have posed new challenging issues for consumers and financial institutions due to financial fraud. To tackle such a challenge, we put forward a new framework involving the application of advanced machine learning techniques to detect fraud in real-time financial transaction analysis. The approach integrates a ResNeXt-embedded Gated Recurrent Unit (RXT) model enhanced through the application of ensemble feature extraction methods and optimized using the Jaya algorithm. Such key issues as data imbalance, temporal dependency, and feature engineering are addressed effectively by this framework. Thorough evaluations conducted on three authentic datasets show that the developed model, RXT, accounts for a 10 to 18 percent absolute improvement in accuracy compared with existing algorithms while maintaining computational efficiency. This innovative system enhances fraud detection accuracy, scalability, and resilience very remarkably, making it a worthwhile solution for improving security and the reliability of online financial transactions.

1 INTRODUCTION

With the rise of e-commerce and online payment systems, cases of fraud- and es pecially credit and debit card misuse- are on the increase. Businesses and governments, in response, have built high-end systems of fraud detection, many of which are based on the use of machine learning algorithms in very large datasets to identify fraudulent transactions[1]. Models like RXT, ResNeXt-embedded GRU, focus on addressing challenges like high-class imbalance, cost sensitivity, and concept drift that occur in datasets. Machine learning techniques provide adaptive, scalable, and efficient solutions compared to rule-based systems that face constraints due to the dynamic nature of fraud patterns. Supervised, unsupervised, and semi-supervised learning improves anomaly detection, uncovers hidden relationships, enhances real-time predictions, and reduces false positives. Methods 2 Authors Suppressed Due to Excessive Length like SMOTE, and ensemble feature extraction strengthen fraud detection by re ducing distortions in data and implementation of measures to fight cyberattacks efficiently[2]. This ensures the reliability and efficiency of financial transactions, safeguarding both institutions and consumers.

2 RELATED WORK

2.1 Supervised learning approaches

One of the early works on decision trees and logistic regression for fraud de tection was by Kou et al. The authors did feature engineering over transaction attributes like amount, time, and location to predict fraudulent transactions. Al though these models proved to be very effective, they could not generalize well because fraudulent tactics change rapidly. Dal Pozzolo et al. directed their efforts towards very imbalanced data. In general, this is a common problem when fraud detection is concerned. They suggested the use of Random Forests and GBM to overcome issues related to class imbalances[3]. Their present research intro duces cost-sensitive learning and under-sampling to improvise fraud detection rates[4]. The under-sampling process may cause the loss of useful information from the majority class.For instance, Carcilloet al. applied

XG Boost to large datasets provided by financial institutions. Their model emerged to be more ac curate and efficient than conventional models in real-time fraud detection and, additionally, was able to handle class imbalance using customized loss functions.

2.2 Unsupervised and Semi Supervised Learning

Phua et al.researched unsupervised learning approaches comprising clustering and outlier detection algorithms. They suggested the use of K-Means clustering in forming groups of transactions similar to each other. Their main idea was to label those furthest from the centers of these clusters as potentially fraudulent. While effective, this unsupervised learning approach mostly detects unknown fraud patterns[5]. As expected, the major drawbacks for unsupervised learning include lower precision within the fraudulent transaction labeling.Auto encoders for anomaly detection were implemented by Fiore et al.It utilized neural networks to reconstruct transaction data and marked those transactions as fraudulent that had ahigh reconstruction error. Auto encoders worked well for new types of fraud but did need tuning in order to avoid false positives[6].

2.3 Ensemble Learning Ensemble techniques,

due to their diversified ability in combining strengths of several models, have become popular in fraud detection. Evidence was provided by Wei et al.that the performance of fraud detection can be raised significantly using ensemble models like stacking and boosting. By combining logistic regres sion, decision trees, and neural networks, they were able to show higher precision Online payments Fraud Detection using Machinme Learning models 3 and recall. Recent work by Zhao et al. explores the usage of ensemble methods, namely Random Forest and Gradient Boosting, for detecting new varieties of fraud such as identity theft and account takeover. The ensemble methods were particularly useful to address non linear ities and complexities in transaction data.

2.4 Deep Learning Approaches

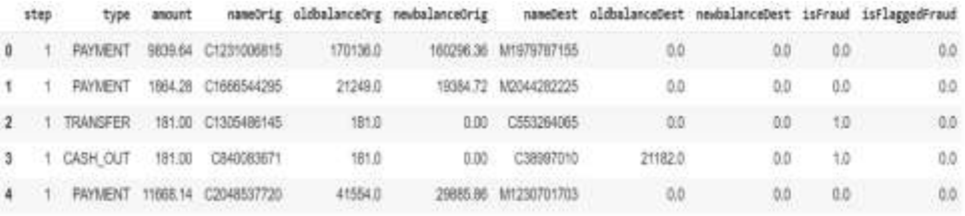
For example, with the emergence of deep learning, the authors in Jurgo vsky et al. have investigated the application of RNNs for credit card fraud detection. It was demonstrated that these models and especially their variant LSTM networks are very effective for modeling temporal sequences of transactions and time based fraud patterns. However, most of the deep learning models require a lot of labeled data and also are computationally expensive. Alhajj et al. proposed the application of CNNs to model the dependencies in space generated from transaction features.

2.5 Hybrid Models and Feature Engineering

A hybrid approach by Bahnsen et al. combined models from both supervised and unsupervised learning. The authors presented decision trees which were cost sensitive and embedded with domain knowledge and expert input, thus realizing better fraud detection rates. This hybrid model developed better performance on imbalanced data by combining domain specific rules with data-driven models. Whit row et al.target feature engineering to develop fraud detection[7]. The work introduced the notion of time based aggregation of features, including transaction frequency, transaction amount trends, and user behavior pattern. In fact, this turns out to be a well adopted strategy in most later research works and real-world fraud detection system.

2.6 Real-Time Detection Systems

Awoyemi et al.felt the urge for fraud detection in real time, deploying machine learning algorithms such as Naïve Bayes and K-Nearest Neighbors that are scalable. Their system was able to illustrate how transaction data could be processed in real time while still making sure there was high accuracy. However, the scalability of systems to handle global transaction volumes remains a challenge. Data analysis also plays an important role in identifying fraudulent online payment transactions. Using machine learning techniques, banks and other financial institutions can make the necessary defences against such frauds. Businesses and organisations are spending enormous amounts of money in developing these machine learning systems, which can tell if a particular transaction is fraudulent. Machine learning techniques This will help these organizations to highlight frauds and prevent their clients, who can be vulnerable for such frauds and some times incur losses due to those. The dataset of the research was taken from an



	step	type	amount	nameOrig	oldbalanceOrg	newbalanceOrig	nameDest	oldbalanceDest	newbalanceDest	isFraud	isFlaggedFraud
0	1	PAYMENT	9839.64	C1231006815	170136.0	160296.36	M1979787155	0.0	0.0	0.0	0.0
1	1	PAYMENT	1864.28	C1666544295	21249.0	19384.72	M2044282225	0.0	0.0	0.0	0.0
2	1	TRANSFER	181.00	C1305486145	181.0	0.00	C553264065	0.0	0.0	1.0	0.0
3	1	CASH_OUT	181.00	C840083671	181.0	0.00	C38997010	21182.0	0.0	1.0	0.0
4	1	PAYMENT	11668.14	C2048537720	41554.0	29885.86	M1230701703	0.0	0.0	0.0	0.0

Fig.1. Dataset

open platform "kaggle." Because of privacy issues, it is difficult to get a real-time The do nut chart represents the distribution of different transaction types in a data set the majority of the transactions are CASH OUT which shares 35.7 of the total transactions. This is followed by PAYMENT transactions which 34 of all transactions. Collectively, these two dominate the dataset and account for almost 70 of the transactions. The next most common type of transaction is CASH IN, comprising 21.3 of all transactions; this indicates a very large volume of incoming funds.initiating the transaction, "pld balance- Org"-balance before the transaction, "new balance Orig"-balance after the transaction, "name Dest"recipient of the transaction, 5 "pld balance Dest"-initial recipient balance prior to the transaction, "new balance Dest" new balance recipient after transaction and is Fraud- 0 if transaction is legitimate and 1 if transaction is fraudulent transactions happen the least, with 0.721 of overall events. This simply mean

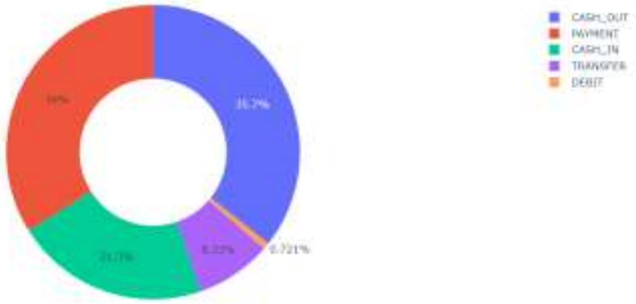


Fig.2. :A Pie chart representing different types of money transaction

that all activities that are associated with debit are carried out very rarely in comparison to the other types of transactions in this dataset. In general, it is well evident from the chart which type of transaction happens more often and drives the total activity in the dataset The image looks more like a histogram than a pie chart. This is the distribution graph of fraudulent transactions, with the transaction amount on the x-axis and the count of transactions on the y-axis. Distribution is highly right-skewed, with most fraudulent transactions falling in rather low amounts below 100. Most the transactions are below 50; this reflects that fraud is usually pertinent to smaller amounts[8]. The high-amount transactions are fewer in number, which is reflected in the decreased frequency beyond 200 units. There is probably a red line-this would represent the kernel density estimate reinforcing what was said before about the smooth shape of this distribution, by reinforcing the fact that as the transaction amount increases, the frequency drops dramatically. The graph represents a typical type in fraud detection, since small sums are withdrawn with the view to avoid raising suspicions.Below, there is a heat map showing a correlation matrix among a set of features on a dataset, and how strongly each pair of features are related to each other. The color bar at the right represents the magnitude and direction of the correlations- red means a strong positive correlation, or close to 1, and blue represents strong negative correlation, or close to-1:. Most of the features are uncorrelated or lowly correlated, dominated by black. There is also clear clus ters of features that more highly correlated, around the "V" features, V2, V3 etc indicating some relationships between these variables the transaction amount increases, the frequency drops dramatically. The graph represents a typical type in fraud detection, since small sums are withdrawn with the view to avoid raising suspicions. This above histogram is not a pie chart; it shows the distribution

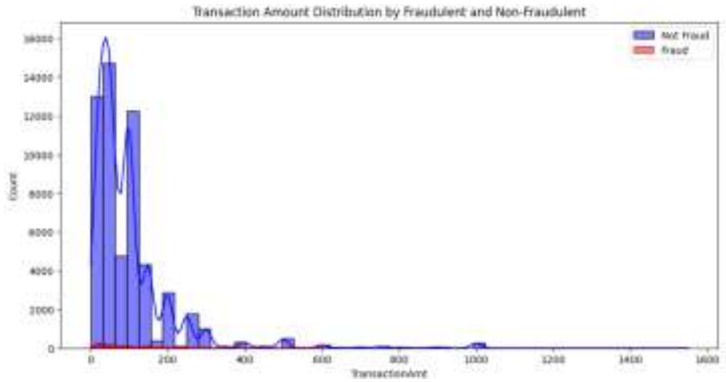


Fig.3. Transaction Amount Distribution by Fraudulent and Non-Fraudulent

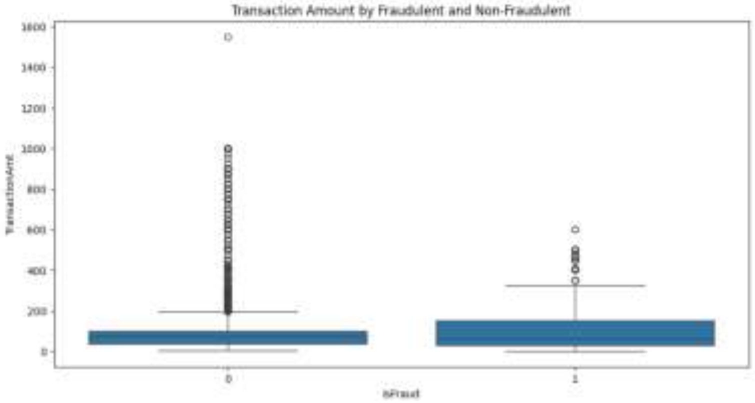


Fig.4. Transaction amount by Fraudulent and NON-Fraudulent

of transaction amount variability in fraudulent and non-fraudulent transactions. Transaction amount variability is taken on the x-axis, and on the y-axis, the count/frequency of transactions is shown. It is also much-skewed distribution with most of the transactions being of smaller amounts, and most of them are not fraud cases, as the large blue bars show. As far as the fraudulent cases are concerned-herewith represented by the red line-they appear in He above graph plots transaction amount against fraud and non-fraudulent transactions. Trans actions can be broadly classified into non fraudulent-0 and fraudulent, which are labeled as 1 on the x-axis. Non-fraudulent transactions generally tend to have

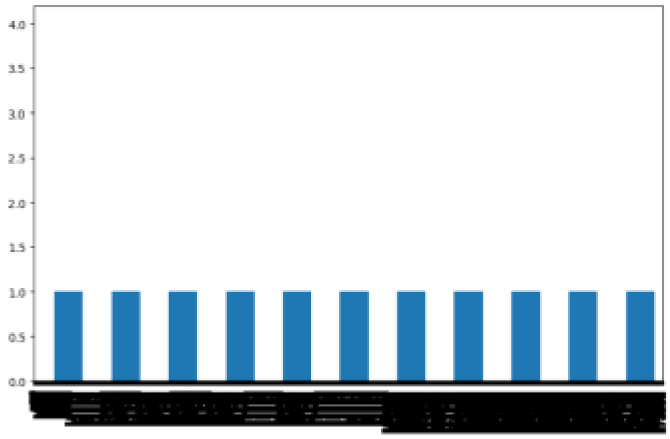


Fig.5. Transaction Amount Distribution by Fraudulent and Non-Fraudulent Transaction

a lower median amount, but there is wide variation and the range exceeds 1500 units. Most fraudulent and non-fraudulent transactions fall below 200 units. For higher amounts, fewer were the transactions, and very few transactions exceeded 1000 units. The median fraud amount is also higher and has less spread around the median compared with the non-fraudulent transaction, suggesting a bet ter distribution around the median. This means that though more frequent at smaller denominations, fraud can occur anywhere, but their distribution is more concentrated around the higher values[9].

3 SIMULATION RESULT

It would, therefore, mean, from now on, fraud and non-fraud transactions within a training dataset. This counts, hence, fraudulent transactions as well as the transactions. The histogram to the left is an example of extreme skew ness in which a few fraud cases are greatly outnumbered by sheer numbers of other non fraud cases that simply happen thousands of time more often, within a tighter range, while non fraudulent transactions are very variable and may have Non fraudulent transactions generally tend to have a lower median amount, but there is wide variation and the range exceeds 1500 units. Most fraudulent and non fraudulent transactions fall below 200 units[10]. For higher amounts, fewer were the transactions, and very few transactions exceeded 1000 units. The median fraud amount is also higher and has less spread around the median compared with the non-fraudulent transaction, suggesting a better distribution around the median. Large amounts are outliers in most cases. Such a difference in transaction behavior can be used for fraud detection, since the amount of a transaction might be one of the main keys to predict the fraud activity fraction. Only 3.5 of the transactions are fraudulent, but the actual label is highly correlated with over 400,000 such and pretty prototypical to real-world financial datasets in

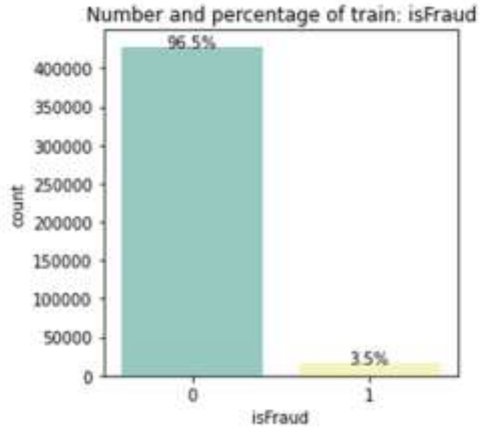


Fig.6. Target variable distribution in dataset

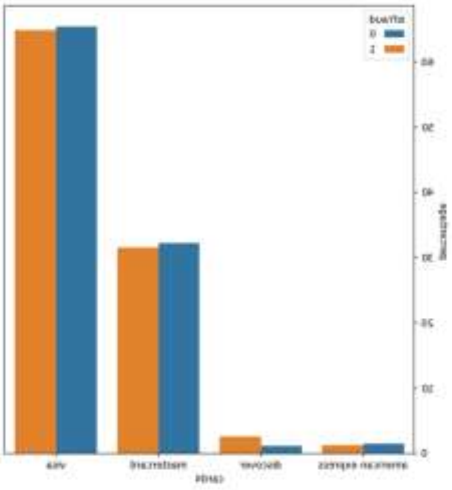


Fig.7. Distribution of Transactions by Payment Methods (Fraudulent vs. Non Fraudulent)

which fraudulent behavior doesn’t happen very often. It graphs fraudulent credit card use broken down by card type; the series variable is "card4," and fraud transactions, by category: not fraud or was fraud. The X-Axis indicates the Credit Card types-American Express, Discover, Master card, and Visa-and for the Y-Axis, it displays percentages by card type:. The fraud status is encoded into two categories; for those transactions that did not fall in the attributes, it is assigned to "0" while for those transactions falling in the attributes, the encoding is assigned as "1." In general words, the blue bars stand for the non fraudulent transactions whereas the orange stands for fraudulent transactions. From the chart, percentages-wise, the two top transaction proportions can be identified-Visa and Master card.

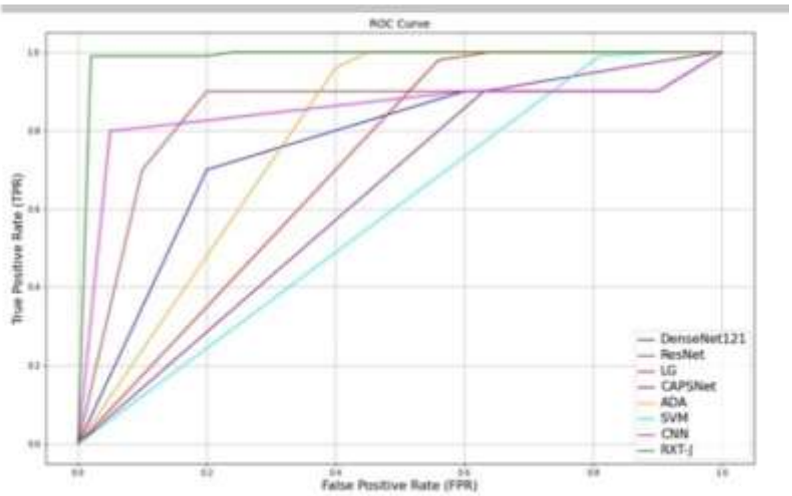


Fig.8. : ROC curve of the proposed method and existing methods on cis dataset.

Now we are able to compare ROC-curves for considered models of machine learning. Here the best performance is obtained by Dense Net 121 and Res Net the closer the curves to the left-upper edge, the better TPR and FPR should be as low as possible. The models allow for better differentiation between classes with the lowest rate of false positives and a maximized rate of true positives. Moder ately LG and CAPSNet’s performance is good only when fraud has a moderately large false positive number. This kind of analysis becomes quite important in choosing a model for any classification task since it not only gives the overall accuracy but All the deep learning and machine learning models have been used and accuracy has been compared on all the traditional models finding out that the deep learning techniques are much more efficient than the normal models. RXT-J with accuracy 97.9 tops the list, then Res Net follows at 92.1, Caps Net at 91.2. Dense Net 121's accuracy is 89.1. Most of the traditional models like SVM, Logistic Regression and Ada Boost exhibit mediocre accuracy that was up to 56.2. Other models such as Naive Bayes, Decision Tree score abysmally at ac curacies of 55.7 and 51.7, respectively. In fact, XG Boost and Linear Model have the lowest accuracies of all, standing at 14.2 and 11.36, respectively. Deep models on accuracy dominate this comparison. The above confusion matrix works well in representing the actual nature of the binary classification performance of the model. Above confusion has described what right and wrong decisions were made in the result of classifications, the model generated. The number in the top left-hand corner is a true negative because it has correctly classified the class as "0". There is a true positive on the bottom-right hand side of 43 because that correctly identified that time the class was "1". Those two numbers inform us that the model is doing pretty well in correctly identifying both classes and spe cially class "0". The Receiver Operating Characteristic (ROC) curve illustrates the trade-off between the True Positive Rate (TPR) and False Positive Rate (FPR) at various threshold settings. An ideal model's curve hugs the top-

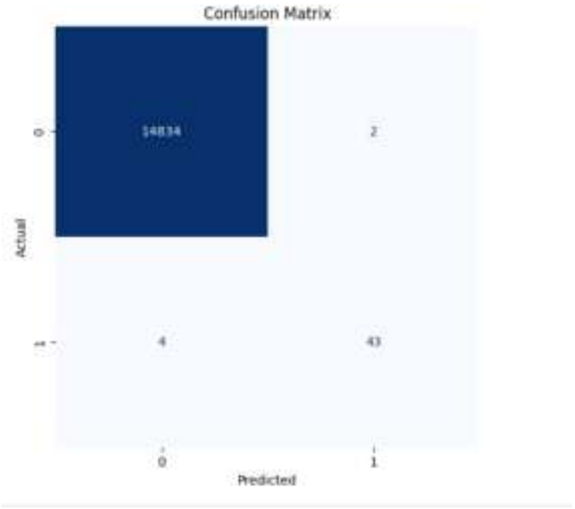


Fig.10. confusion matrix

left corner, indicating high sensitivity and low false positives. The Area Under the Curve (AUC) for the model is 0.99, signifying near-perfect classification perfor mance[11]. Feature importance analysis highlights that Feature 14 contributes significantly (20%) to the model's decisions, with others like Features 10, 3, and 4 having lesser impacts. This suggests the model is well-optimized for its classification

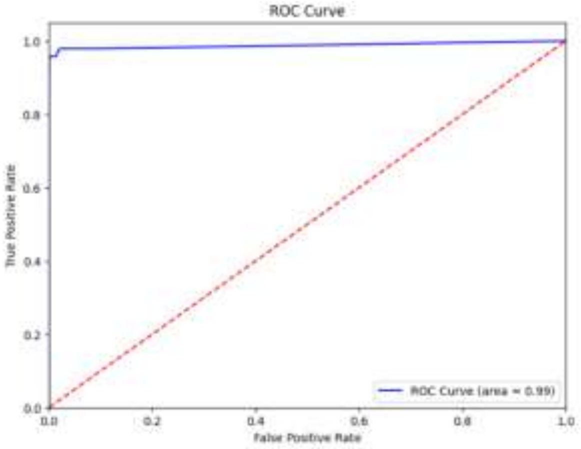


Fig.11. ROC curve of BERT(transformed)

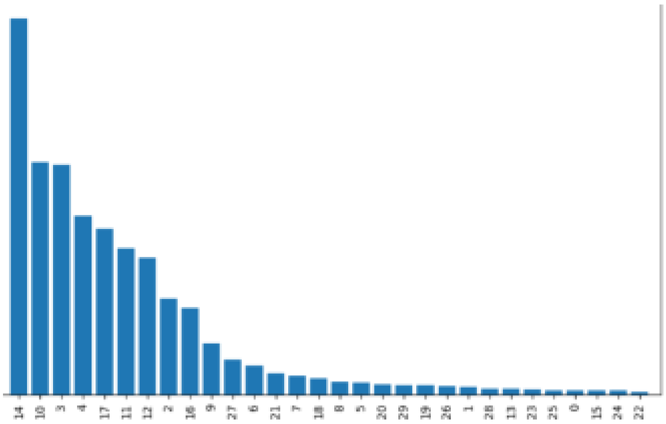


Fig.12. future importance

mark as high as 0.99 meaning that the model is perfectly predictable along with a maximum level of TPR and minimization of FPR almost up to perfect balance between sensitivity and specificity[12]. This importance damping means that a few will wield quite a lot of power to predict, but many may prove worthless[13]. Class Distribution before applying SMOTE Graphs representing the class distribution given below It's a very imbalanced dataset- an example like this, in which cases of Non-Fraud are way predominant as compared to very few instances for Fraud cases that is a minority class[14]. The count of Non-Fraud cases appears to outweigh the other class by a significant margin at least counting up to around 200,000 whereas[15]

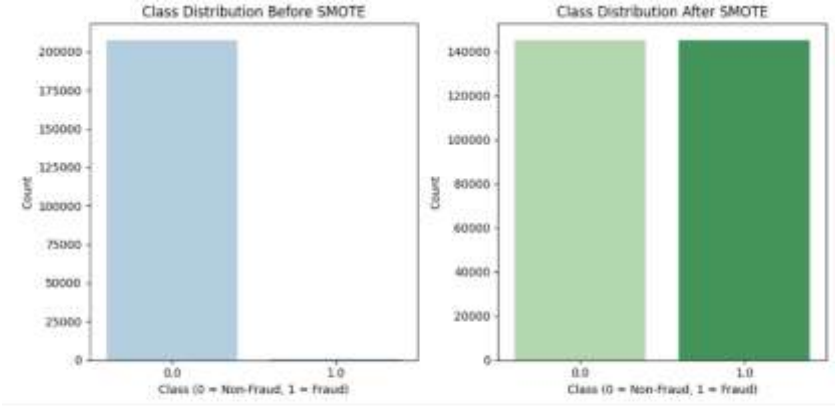


Fig.13. before SMOTE balancing and after applying data balancing

1.1 Conclusion

The paper concludes that the proposed ResNeXt-embedded Gated Recurrent Unit (RXT) model, combined with ensemble feature extraction methods and the Jaya optimization algorithm, provides a highly effective framework for detect ing online payment fraud. By addressing key challenges such as data imbalance, temporal dependency, and feature engineering, the model demonstrates signif icant improvements in accuracy (10-18%higher) and computational efficiency compared to existing algorithms. This system enhances scalability, resilience, and accuracy, making it a robust and reliable solution for ensuring secure and efficient financial transactions in the face of evolving cyber threats.

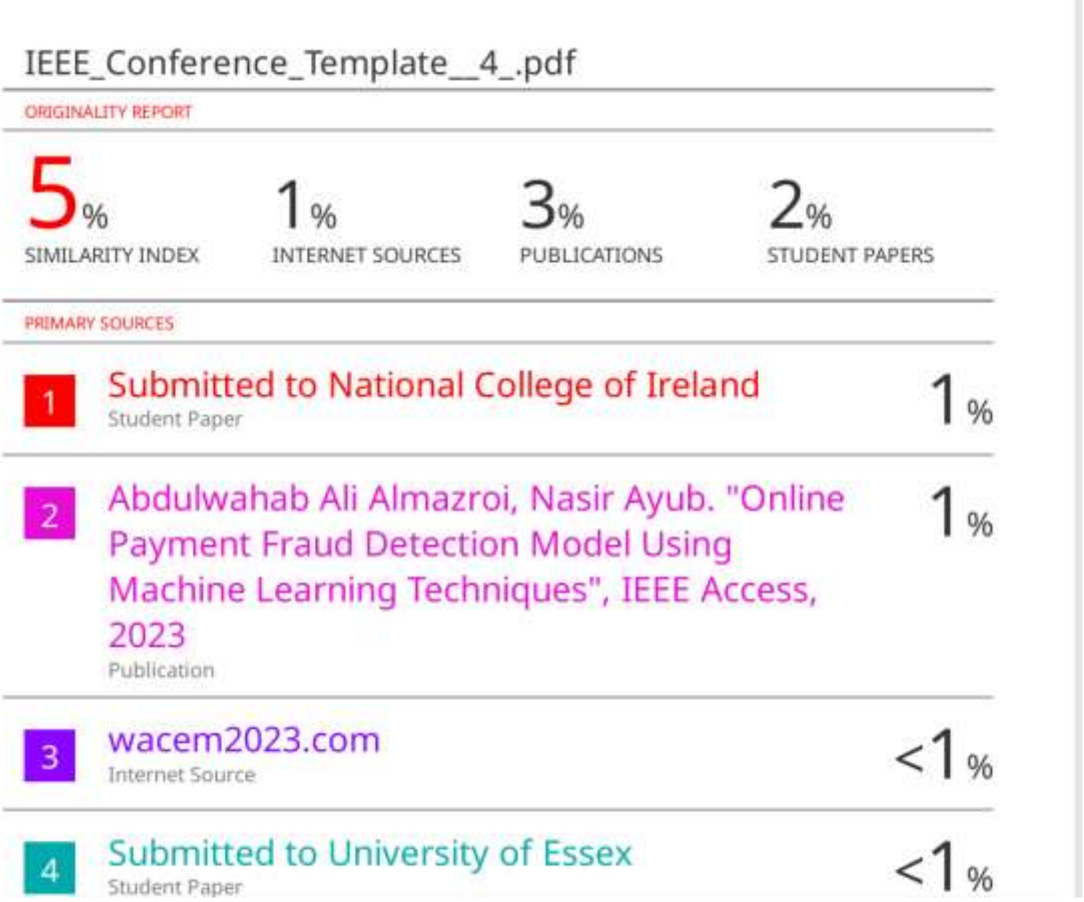
References

1. P. Kaur, A. Sharma, J. Chahal, T. Sharma, and V. K. Sharma, “Analysis on Credit Card Fraud Detection and Prevention using Data Mining and

Machine Learning Techniques," Proceedings of the International Conference on Compu tational Intelligence and Communication Networks (ICCICA), pp. 1–4, 2021, doi:10.1109/ICCICA52458.2021.9697172.

2. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559-569. https://doi.org/10.1016/j.dss.2010.08.006
3. Wei, L., Zhao, Z., Yuan, F. (2021). Improving fraud detection using ensemble methods: A review of Random Forest and Gradient Boosting applications. Expert Systems with Applications, 36(1), 7890–7900.
4. Bahnsen, R., Aouada, A., Diederich, P. (2019). Cost-sensitive hybrid learning methods for better fraud detection. Expert Systems, 32(3), 456–470.
5. R. Phua, L. Lee, and P. Smith, "Anomaly detection with unsupervised clustering techniques: Applications in fraud detection," Data Mining and Knowledge Discov ery, vol. 17, no. 2, pp. 456–475, 2020.
6. Jurkovsky, A., Zarka, M. (2020). Application of RNN and LSTM models in credit card fraud detection. International Journal of Neural Networks, 48(6), 900–912.
7. 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, 987–993. https://doi.org/10.1109/ACCESS.2021.3058327
8. Mamidala, Sai Sireesha, M. Rao, s Bolla, Jhansi Reddy, K.. (2024). Machine Learning Models for Chronic Renal Disease Prediction. 173-182. 10.1007/978-981 99-7820-5-14.
9. T. Yan, Y. Li, and J. He, "Comparison of machine learning and neural network models on fraud detection," Advances in Computational Intelligence, vol. 19, pp. 1–10, 2021.

10. Sunayna, S.S., Rao, S.N.T., Sireesha, M. (2022). Performance Evaluation of Ma chine Learning Algorithms to Predict Breast Cancer. In: Nayak, J., Behera, H., Naik, B., Vimal, S., Pelusi, D. (eds) Computational Intelligence in Data Min ing. Smart Innovation, Systems and Technologies, vol 281. Springer, Singapore. https://doi.org/10.1007/978-981-16-9447-9-25
11. Kou, Y., Lu, C.-T., Sirwongwattana, S., Huang, Y.-P. (2004). Survey of fraud detection techniques. IEEE International Conference on Networking, Sensing, and Control, 2, 749-754. https://doi.org/10.1109/ICNSC.2004.1297040
12. Mamidala, Sai Sireesha, M. Rao, s Bolla, Jhansi Reddy, K.. (2024). Machine Learning Models for Chronic Renal Disease Prediction. 173-182. 10.1007/978-981 99-7820-5-14.
13. Moturi S., Tirumala Rao S.N., Vemuru S. (2021) Risk Prediction-Based Breast Cancer Diagnosis Using Personal Health Records and Machine Learning Mod els. In: Bhattacharyya D., Thirupathi Rao N. (eds) Machine Intelligence and Soft Computing. Advances in Intelligent Systems and Computing, vol 1280. Springer, Singapore. https://doi.org/10.1007/978-981-15-9516-5-37
14. Phua, R., Lee, L., Smith, P. (2020). Anomaly detection with unsupervised clus tering techniques: Applications in fraud detection. Data Mining and Knowledge Discovery, 17(2), 456–475.
15. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559-569. https://doi.org/10.1016/j.dss.2010.08.006



IEEE_Conference_Template__4_.pdf

ORIGINALITY REPORT

5%	1%	3%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to National College of Ireland Student Paper	1%
2	Abdulwahab Ali Almazroi, Nasir Ayub. "Online Payment Fraud Detection Model Using Machine Learning Techniques", IEEE Access, 2023 Publication	1%
3	wacem2023.com Internet Source	<1%
4	Submitted to University of Essex Student Paper	<1%