Grenze International Journal of Engineering and Technology, January Issue

Machine Learning based Real Time Fraud Detection: Tackling Imbalanced Data with Gradient Boosting Techniques

Archana Sasi[1], Muhammad Saalim[2], Nikil Basil Shibu[3], Gauri Jaiswal[4], Pearl Ishika Taide[5] and Shibin Shereef[6]
[1-6]Department of Computer Science and Engineering, Faculty of Engineering and Technology, Jain University, Bengaluru, Karnataka, India
Email: archana.sasi2k8@gmail.com, saalimmomin12, nikilshibu01, gauri082005, ishikataide3, shibinshereef03@gmail.com

***Abstract*— The rise of electronic payment systems has revolutionized the financial sector but has also led to a surge in credit card fraud, imposing significant barriers for banking institutions and individuals. This study focuses on the development of real-time credit card fraud detection systems using advanced Machine Learning (ML) techniques, particularly Gradient Boosting methods such as XGBoost, LightGBM, and CatBoost. These models are well-known for their strong predictive accuracy and inherent capability to address class imbalance through weighted loss functions and regularization. One of the key barriers in fraud detection is the highly imbalanced nature of transaction datasets, which can hinder model performance. To mitigate this, the study integrates strategic feature engineering and interpretability tools to enhance the detection of anomalous transaction patterns. The system's effectiveness is assessed by using performance metrics such as precision, recall, and F1-score. Outcomes indicate that gradient boosting models outperform traditional methods like logistic regression and random forests, particularly in minimizing false negatives crucial in fraud prevention. The proposed approach strikes a balance between computational efficiency and real-world applicability, making it a viable solution for scalable, high-dimensional fraud detection environments.**

***Index Terms*— Fraud detection, Gradient Boosting, Machine Learning, Precision, Recall.**

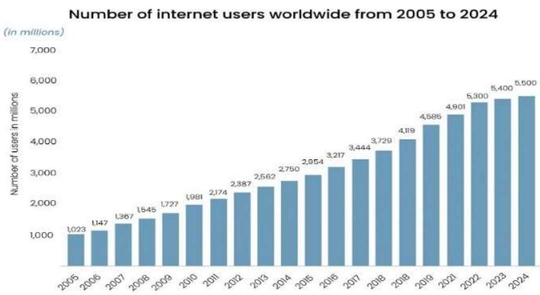
I. INTRODUCTION

Technology advancements have resulted in broad usage of facilities such as electronic commerce, tap-and-pay, and digital bill payment methods. As these online payment options become more prevalent, the incidence of online fraud has risen significantly. This increase in fraudulent activities has prompted extensive research into analyzing and sensing fraud in online transactions over the application of various techniques.

The current research focuses on discovering credit card fraud by employing ML techniques, with the goal of predicting fraudulent transactions with the highest possible accuracy. The objective is to create a robust Deep Learning (DL) model that can precisely identify whether a transaction via credit card is fraudulent or not. Figure 1 shows the growth of internet that leading to numerous frauds. The aim of such fraud is often to obtain goods without payment or to acquire unauthorized funds. Credit cards, in particular, are appealing targets for fraudsters because they enable the rapid acquisition of substantial amounts of money with relatively low risk.

Grenze ID: 01.GIJET.12.1.344_1

Figure 2 illustrates a bar graph that clearly depicts the simultaneous rise of internet users and the world population over 10 years [1]. A significant portion of these fraud cases occur on e-commerce sites. In the current generation, people prefer shopping online rather than going to physical stores. This trend has led to the rapid growth of e-commerce sites, which in turn has increased the risk of credit card fraud. To mitigate such fraud, it is vital to identify and implement the most efficient algorithm for reducing fraudulent use of credit cards. In accordance with 'U.K. Finance' [2], forged transactions linked to credit and debit cards represent a significant source of financial damage in the banking sector. The rapid growth in technology has exacerbated this risk, resulting in substantial monetary losses on a global scale. Hence, there is an urgent need to implement robust credit card fraud detection measures to mitigate financial losses and safeguard the integrity of financial systems worldwide. In the last few years, the surge in credit card fraud detection has garnered significant attention from scholars and researchers [3].



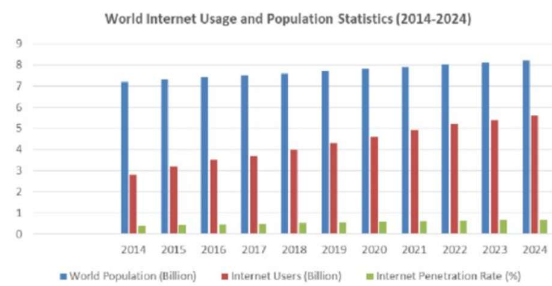


Figure 1. Growth of the internet from 2005-2024 (in millions) Figure 2. Global internet consumption and population estimates (2014–2024)

The current research focuses on discovering credit card fraud by employing ML techniques, with the goal of predicting fraudulent transactions with the highest possible accuracy. The objective is to create a robust Deep Learning (DL) model that can precisely identify whether a transaction via credit card is fraudulent or not. Figure 1 shows the growth of internet that leading to numerous frauds. The aim of such fraud is often to obtain goods without payment or to acquire unauthorized funds. Credit cards, in particular, are appealing targets for fraudsters because they enable the rapid acquisition of substantial amounts of money with relatively low risk.

Figure 2 illustrates a bar graph that clearly depicts the simultaneous rise of internet users and the world population over 10 years [1]. A significant portion of these fraud cases occur on e-commerce sites. In the current generation, people prefer shopping online rather than going to physical stores. This trend has led to the rapid growth of e-commerce sites, which in turn has increased the risk of credit card fraud. To mitigate such fraud, it is vital to identify and implement the most efficient algorithm for reducing fraudulent use of credit cards. In accordance with 'U.K. Finance' [2], forged transactions linked to credit and debit cards represent a significant source of financial damage in the banking sector. The rapid growth in technology has exacerbated this risk, resulting in substantial monetary losses on a global scale. Hence, there is an urgent need to implement robust credit card fraud detection measures to mitigate financial losses and safeguard the integrity of financial systems worldwide. In the last few years, the surge in credit card fraud detection has garnered significant attention from scholars and researchers [3].

In this study we implement three different Gradient boosting algorithms, and compare the results of the three algorithms using confusion matrix. Gradient boosting algorithms work very well with imbalance data sets, therefore making it an optimal algorithm for identification of credit card fraud. As fraudulent transactions are very rare, therefore making the datasets highly imbalanced. Those boosting algorithms use different methods to handle the imbalance, and generate the output.

II. RELATED WORK

With the increased usage of credit cards and electronic payments, fraudulent use of credit cards is now a serious concern worldwide. As fraudsters keep changing their methods, researchers are constantly exploring smarter ways to catch these suspicious transactions early. In recent years, ML and DL have become popular tools in this fight. Techniques like Random Forest (RF), Decision Trees (DT), Logistic Regression (LR), Naïve Bayes (NB), and Support Vector Machines (SVM) are commonly used to spot fraud patterns automatically. Since forged transactions are much less common than valid ones, most studies rely on resampling techniques like Synthetic Minority Over-Sampling Technique (SMOTE) and under-sampling to fix the imbalance in data. Researchers also use a mix of evaluation metrics like accuracy, precision, recall, and F1-score to judge how well their models perform. Overall, the latest research shows that combining multiple models (ensemble learning) and balancing the dataset properly leads to much better fraud detection results.

The paper by Ananya Sarker et al. [4] explores different ML methods to identify illegal credit card payments. The authors tested four models: RF, DT, NB, and SVM. The study highlights the challenge of detecting fraud as fraud patterns change frequently. The dataset used comprised 284,807 transactions, of which only 492 were fraudulent, making it highly imbalanced. The authors applied sampling techniques to address this issue. Among the models tested, RF performed the best, achieving 99.96% accuracy with high precision and recall. DT also performed well, while NB and SVM showed lower accuracy due to their sensitivity to imbalanced data. The paper by Thirunavukkarasu M. et al. [5] explores different ML methods to identify illegal credit card transactions. The authors used RF and DT algorithms to categorize transactions as fake or authorized. The study highlights the increasing risk of credit card theft and the need for advanced detection approaches. With criminals constantly changing their techniques, ML provides an efficient way to automate fraud detection. The RF algorithm was chosen because it performs well on large datasets, reduces overfitting, and provides high accuracy. The authors collected transaction data, pre-processed it, and applied feature extraction techniques. The efficacy of the model was assessed using accuracy, sensitivity, specificity, and precision.

The paper by Deep Prajapati et al. [6] explores different ML models to identifies illegal credit card activities. The authors tested RF, XGBoost, and ANN on an extremely unbalanced data collection of payments with credit cards. The study highlights the challenges of fraud detection, as fraudsters constantly change their tactics. The authors used data balancing techniques, including under sampling, oversampling, and SMOTE Tomek, to improve model performance. Among the models tested, RF with SMOTE Tomek balancing performed the best, making it the most effective approach for identifying fraudulent transactions. The study concludes that RF is the most reliable model for fraud detection when combined with the right data balancing techniques. The paper by Siddhant Bagga et al. [7] explores different ML models to identify transactions that are fraudulent. The authors tested logistic regression, K-Nearest Neighbors (KNNs), RF, NB, multilayer perceptron, AdaBoost, quadrant discriminant examination, pipelining, and ensemble learning on an extremely imbalanced collection of data. The study highlights the challenges of fraud detection, as fake transactions frequently resemble valid ones. The dataset used was highly imbalanced, so the authors applied the ADASYN method to balance it before training the models. These models outperformed traditional ML algorithms regarding precision, recall, and F1-score, making them more effective in detecting fraudulent transactions. In their study [8], Khatri et al. analyzed the effectiveness of ML algorithms to determine fraudulent use of credit cards. The authors investigated DT, KNN, LR, RF, and NB. Using an extremely unbalanced sample data generated from European cardholders, the authors evaluated the precision of every ML method as one of the main performance metrics.

In their study [9], Manjeevan et al. developed a sophisticated electronic payment card counterfeiting detection mechanism utilizing the Genetic Algorithm (GA) for feature selection and consolidation. The authors assessed the effectiveness of their recommended strategy by applying numerous ML algorithms. Results indicated that GA combined with RF (GA-RF) with an accuracy of 77.95%, GA combined with ANN (GA-ANN) attained an accuracy of 81.82%, and GA combined with DT(GA-DT) reached an accuracy of 81.97%. Rishikeshan O V et al. [10] introduced an enhanced algorithm for detecting illegitimate credit card, called the NB improved KNN method (NBKNN). They applied this algorithm to a dataset to identify fraudulent transactions effectively. Mohamad Zamini [11] proposed an unsupervised identification of fraud approach using autoencoder-based clustering. An auto-associator neural network, was utilized to reduce dimensionality, retrieve valuable traits, and improve the neural network's effectiveness in learning. Experiments using a European dataset containing 284,807 transactions resulted in a training loss of 0.024, a validation loss of 0.027, and a mean reconstructive error for non-fraudulent data that was 75% lower than the mean reconstructive error. In their study [12], Awoyemi et al. compared diverse ML algorithms employing the European cardholders credit card forgery database. Employing a hybrid sampling technique to address the dataset's imbalanced nature, the authors evaluated the performance of NB, KNN, and LR. Utilizing a Python-based ML framework, experiments primarily focused on accuracy as the important performance metric. While NB and KNN exhibited relatively satisfactory results, the study did not discover the potential implementation of feature selection methods. They also compared different ML methods such as NB, KNN, and LR on a European credit card fraud dataset. They used a hybrid sampling technique to handle data imbalance and evaluated models using accuracy. However, the study didn’t explore feature selection methods.

III. METHODOLOGY

The dataset used in our research contains a total of 100000 credit card transactions. Among which 99000 transactions are legit and 1000 transactions are fraudulent. We also apply SMOTE to balance the dataset. The following section explains the implementation of Boosting methods such XGBoost (Extreme Gradient Boosting), LightGBM (Light Gradient Boosting Machine) and CatBoost [13] [14] [15].

A. XGBoost Classifier

XGBoost is a scalable, effective, and optimized Gradient Boosting Algorithm (GBA) that has expanded substantial popularity in ML due to its excellent performance and capacity to manage large datasets efficiently. XGBoost uses an ensemble of DTs, in which error of previous trees are corrected by new ones that supports missing value handling and can efficiently process large datasets with high-dimensional features. In this method we split the dataset into training and testing sets. We consider 80% of the transactions for the training set and 20% of the transactions for the testing set. Then we use the XGBoost algorithm for training the model. After this we estimated the accuracy, precision, recall and F1-score. We set the learning rate as [0.01, 0.05, 0.1], max depth as [4] [5] [6], and n estimators as [100, 200, 500] out of which the model selects the combination that generates the highest accuracy.

B. LightGBM Classifier

LightGBM is another high-performance GBA designed to be quicker and more efficient, particularly for large datasets. It implements a histogram-based method to accelerate training and reduce memory usage, making it an excellent choice for fraud detection. Unlike level-wise growth in traditional DTs, LightGBM grows tree leaf-wise, improving accuracy and efficiency. It supports categorical feature handling, and handles imbalanced datasets effectively [16]. While applying LightGBM we first splitted the data out of which 80% for training the model and 20% of the data for testing purpose. We also generate a confusion matrix to better comprehend the model. In this model we keep the learning rate as 0.01, number of iterations as 1000 and max depth as 7. We also included other parameters such as number of leaves, feature fraction and bagging fraction.

C. CatBoost Classifier

CatBoost is a high-performance GBA built to handle category features efficiently. It stands out because it does not require extensive preprocessing like one-hot encoding, making it well-suited for datasets with categorical variables. The algorithm automatically processes categorical data, reducing memory usage and training time while improving accuracy. For our fraud detection model, we split the dataset into 80% training data and 20% testing data. The CatBoost classifier is trained using 2000 iterations, a learning rate of 0.05, and a depth of 8 to optimize accuracy.

IV. Result Analysis

The considered dataset includes a total of 100000 transactions among which 1000 transactions are classified as fraudulent transactions. The most fundamental performance indicator is accuracy. One can presume that their model is best if it has a high degree of accuracy, but it is only applicable when the datasets are symmetric and the false positive and false negative values are almost equal. As a result, we need to examine both of the parameters. The following Figure 3, 4 and 5 represents the Confusion Matrix (CM) of the models.

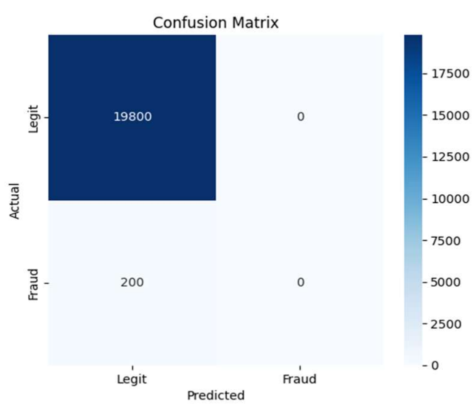


Figure 3. CM for XGBoost

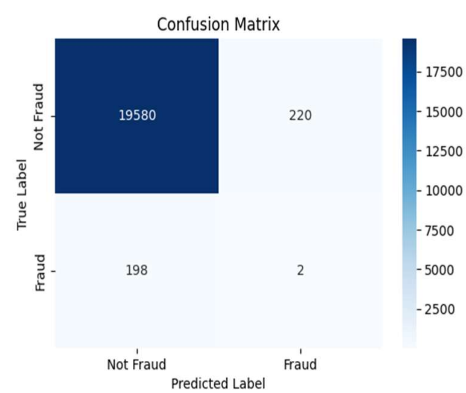


Figure 4. CM for LightGBM

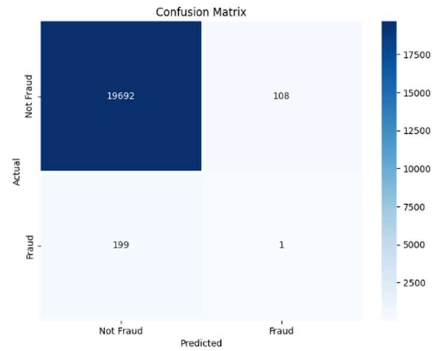


Figure 5. CM for Catboost

This Figure 6 shows how confident the XGBoost model was when predicting fraudulent transactions, represented by the predicted probabilities for the fraud class. Most of the bars are clustered between 0.25 and 0.40, meaning the model generally assigns moderate confidence when it suspects a transaction is fraudulent. This kind of distribution is typical when a model is being cautious, trying not to over-commit to labelling something as fraud unless it's really sure, which can be a good sign of balance between false positives and false negatives. The Figure 7 shows how the LightGBM model assigns probabilities to transactions being fraudulent. The blue area represents the non-fraud cases, which are mostly concentrated at lower probabilities close to 0, meaning the model is very confident that these are legitimate. The red part, although much smaller, shows the predicted probabilities for actual fraud cases.

Figure 8 shows how the CatBoost model predicts the probability of fraud for each transaction. Most of the predictions for non-fraudulent transactions (shown in blue) are clustered toward the lower end of the probability scale, meaning the model is very confident that they're not fraud. The fraudulent transactions (in red) are much fewer and mostly overlap with the low probability range, which suggests that even actual frauds are being predicted with low confidence. This implies that CatBoost, while good at identifying non-fraud cases, is still struggling to strongly separate fraud cases from the rest, likely due to the imbalanced nature of the dataset where frauds are rare and subtle.

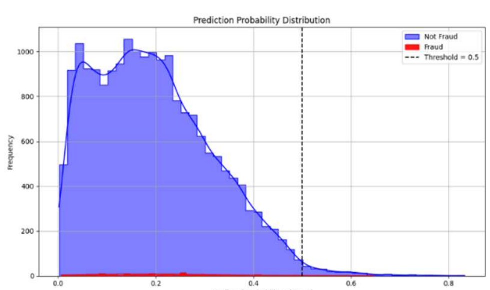


Figure 6. Prediction Graph for XGBoost

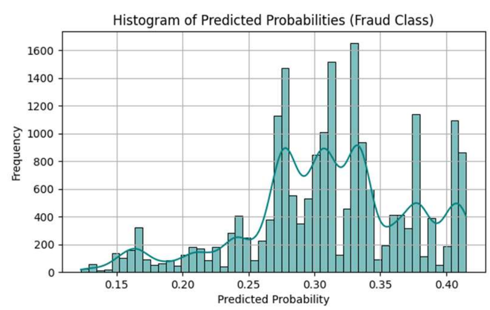


Figure 7. Prediction Graph for LightBoost

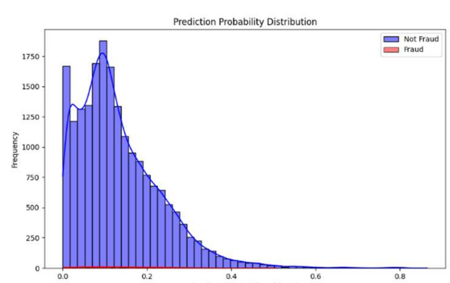


Figure 8. Prediction Graph for CatBoost

The Table 1 below tells us about the performance of the three used models by means of different performance metrics. Among which XGBoost achieved the highest accuracy of 99%. Whereas not much deflection is seen in the other parameters of the three models. Figure 9 shows the comparison graph for all models.

TABLE I. ACCURACY, PRECISION, RECALL AND F1-SCORE OF THE IMPLEMENTED MODELS

Model	Accuracy (%)	Precision	Recall	F1-score
XGBoost	99.00	0.99	1.00	0.99
LightGBM	97.91	0.99	0.99	0.99
CatBoost	98.47	0.99	0.99	0.99

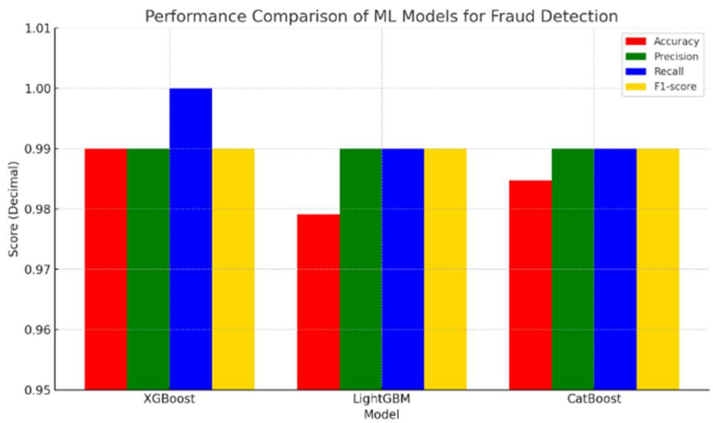


Figure 9. Comparison Graph for all Models

V. CONCLUSION AND FUTURE WORK

In our study, we discovered the effectiveness of three powerful GBAs - XGBoost, LightGBM, and CatBoost for identification of credit card fraud forgery. Working with a highly imbalanced dataset, we implemented SMOTE to balance the data and ensure fair model training. Each model was assessed by means of standard metrics like accuracy, precision, recall, and F1-score, offering a comprehensive understanding of their performance. Among the models, XGBoost showed the highest overall accuracy and recall, making it particularly effective in identifying fraudulent transactions with minimal false negatives. LightGBM and CatBoost also performed competitively, demonstrating the strength of gradient boosting methods in handling complex real-world fraud detection problems. Our findings highlight the importance of using robust models that can adapt to imbalanced datasets and still deliver accurate results. This approach ensures better detection of fraud without sacrificing the reliability of the system. While no model is perfect, the results reinforce that with proper tuning and preprocessing, ML techniques can show a vital role in developing real-time fraud detection systems that are both efficient and trustworthy.

Looking ahead, this work sets a foundation for further enhancement. Future improvements could involve incorporating DL methods, real-time feedback systems, and deploying these models in dynamic environments to evaluate their adaptability. Additionally, introducing explainability techniques can help build user trust by making predictions more transparent. As financial fraud becomes more sophisticated, our detection methods must evolve as well constantly learning, adapting, and improving to meet tomorrow’s challenges. By blending data science with practical application, we move closer to creating intelligent systems that can help protect not just transactions, but the trust users place in digital financial platforms.

ACKNOWLEDGMENT

First and foremost, we are thankful to God Almighty for enabling us to successfully complete this research on schedule. For the chance to conduct this study and for creating a setting that encourages learning and creativity, we are extremely grateful to Jain University, Bangalore. We would like to express our gratitude to Dr. Archana Sasi of the Department of Computer Science and Engineering at Jain University in Bangalore for her significant advice and inspirational leadership. We extend our thanks to our friends for their consistent encouragement and support in launching this effort.

REFERENCES

[1] Tripathy, Sudhanshu Sekhar. "A comprehensive survey of cybercrimes in India over the last decade." In; International Journel of Science and Research, DOI: https://doi.org/10.30574/ijsra.2024.13.1.1919

[2] U.K. Finance. (2023). Fraud the facts 2023: The definitive overview of payment industry fraud. https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2023

[3] Zhu H, Liu G, Zhou M, Xie Y, Abusorrah A, “Kang Q. Optimizing weighted extreme learning machines for imbalanced classification and application to credit card fraud detection.” Neurocomputing. 2020;407:50–62. https://doi.org/10.1016/j.neucom.2020.04.078

[4] A. Sarker et al., Credit Card Fraud Detection Using Machine Learning Techniques, [2024]. Compared Logistic Regression, SVM, and Random Forest; Random Forest achieved the highest accuracy (99.93%), precision, recall, and F1-score.

[5] T. Thirunavukkarasu et al., Credit Card Fraud Detection Using Machine Learning, [2021]. Evaluated Decision Trees, XGBoost, and Random Forest; Random Forest showed superior performance (99.93% accuracy, 99.5% precision).

[6] D. Prajapati et al., Credit Card Fraud Detection Using Machine Learning, [2021]. Tested XGBoost, ANN, and SMOTE-balanced Random Forest; Random Forest with SMOTETomek yielded 99.96% accuracy and 100% precision

[7] S. Bagga et al., “Credit Card Fraud Detection Using Pipelining and Ensemble Learning”, [2020]. Compared AdaBoost, KNN, and pipelining; Pipelining achieved 99.9999% accuracy, outperforming all ensemble methods.

[8] Khatri S, Arora A, Agrawal AP. “Supervised machine learning algorithms for credit card fraud detection: a comparison.”In: 10th international conference on cloud computing, data science & engineering (Confuence); 2020. p. 680-683

[9] Manjeevan, G., Herath, H. M. H. J. K., & Wijesundara, C. S. (2020). Electronic payment card fraud detection using genetic algorithm. 2020 5th International Conference on Information Technology Research (ICITR), IEEE, 1–6. https://doi.org/10.1109/ICITR51264.2020.9375712

[10] Rishikeshan, O. V., Divya, M., & Sruthi, P. (2020). Credit card fraud detection using hybrid machine learning model. International Research Journal of Engineering and Technology (IRJET), 7(6), 6109–6112.

[11] M. Zamini, "An Unsupervised Fraud Detection Method Based on Autoencoder-Based Clustering," IEEE Access, vol. 8, pp. 115066–115080, 2020, doi: 10.1109/ACCESS.2020.3004150.

[12] Awoyemi JO, Adetunmbi AO, Oluwadare SA. “Credit card fraud detection using machine learning techniques: a comparative analysis.” In: International conference on computer networks and Information (ICCNI); 2017. p. 1-9.

[13] T. Thamaraimanalan, A. Haldorai, G. Suresh, and A. Sasi, "Hybrid machine learning methodology for real-time quality of service prediction and ideal spectrum selection in CRNs," Journal of Machine and Computing,2025, DOI: 10.53759/7669/jmc202505099

[14] Alanya-Arango, Javier, Joel Alanya-Beltran, Sathish Kumar Ravichandran, Barinderjit Singh, Archana Sasi, and Durgaprasad Gangodkar. "Internet of Things and Machine Learning based Intelligent Irrigation System for Agriculture." In 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), pp. 67-72. IEEE, 2022.

[15] Vaishnavi, T. and S, Krishnaveni and N, Aravindprakash and S, Akilesh and A C, Hari Prakash, Detection of Credit Card Fraud Using Machine Learning (November 15, 2024). Proceedings of the 3rd International Conference on Optimization Techniques in the Field of Engineering (ICOFE-2024)

[16] Chen, W., Yang, K., Yu, Z. et al. A survey on imbalanced learning: latest research, applications and future directions. Artif Intell Rev 57, 137 (2024). https://doi.org/10.1007/s10462-024-10759-6