ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct1616

Adaptive Fraud Detection: A Machine Learning Framework Combining Supervised and Unsupervised Learning Techniques

Harsh Raj[1]; Deepanshu Chaudhary[2]; Jitendra Singh[3]

[1]SSCSE, Department of CSE Sharda University Greater Noida, Uttar Pradesh, India
[2]SSCSE, Department of CSE Sharda University Greater Noida, Uttar Pradesh, India
[3]Assistant Professor, SSET, Department of CSE Sharda University Greater Noida, Uttar Pradesh, India

Publication Date: 2025/11/15

Abstract: The widespread use of credit cards in financial transactions has significantly increased the risk of fraudulent activities. Detecting fraud in real time is a critical challenge due to the highly imbalanced nature of transaction datasets and the continuous adaptation of fraud strategies. This paper presents a comprehensive study of machine learning techniques for credit card fraud detection. The methodology includes dataset preprocessing, feature engineering, handling of class imbalance, and the application of both supervised and unsupervised learning algorithms. Models including Logistic Regression, Decision Tree, Random Forest, Gradient Boosting, and Autoencoders were evaluated using performance measures such as Precision, Recall, F1-Score, and PR-AUC. Results indicate that Gradient Boosting achieves the most effective balance between fraud detection and false alarm reduction, while Autoencoders are effective in identifying emerging fraud patterns. The study emphasizes the importance of combining supervised and unsupervised methods for robust fraud detection and concludes with recommendations for future enhancements in real-world systems.

Keywords: *Credit Card Fraud, Machine Learning, Imbalanced Learning, Ensemble Models, Anomaly Detection.*

How to Cite: Harsh Raj; Deepanshu Chaudhary; Jitendra Singh (2025) Adaptive Fraud Detection: A Machine Learning Framework Combining Supervised and Unsupervised Learning Techniques. *International Journal of Innovative Science and Research Technology*, 10(10), 3222-3227. https://doi.org/10.38124/ijisrt/25oct1616

I. INTRODUCTION

In today's digital economy, credit cards are one of the most commonly used payment methods worldwide. With the growth of online shopping, e-commerce platforms, and cashless transactions, the convenience of credit cards has also opened doors for fraudulent activities. Credit card fraud not only causes massive financial losses but also damages consumer trust and burdens financial institutions with fraud management costs. Traditional fraud detection techniques often fail to identify evolving fraud strategies, especially in real-time transaction environments.

To address this challenge, we present a machine learning– based fraud detection framework that leverages Artificial Intelligence (AI) and advanced analytics to identify suspicious activities. By analyzing historical transaction data, behavioral patterns, and anomalies, the system provides a proactive defense against fraudulent activities while minimizing disruptions to legitimate customers. This paper explores the role of AI in fraud detection, the core features of the fraud detection system, and its practical applications across the financial sector.

II. LITERATURE SURVEY

Table 1 Literature Survey

Ref	Authors	Approach / Model	Key Contributions	Limitations/ Challenges
[1]	Bolton & Hand (2002)	Statistical / Rule-Based Methods	One of the earliest surveys on fraud detection using statistical models and expert rules.	Inflexible; unable to adapt to new fraud strategies.
[2]	Bhattacharyya et al. (2011)	Logistic Regression & Decision Trees	Demonstrated classical supervised learning methods for fraud detection with interpretability.	Struggled with extreme class imbalance.
[3]	Phua et al. (2010)	Data Mining & ML	Comprehensive review of data	Lacked focus on real-time

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct1616

		Review	mining methods in fraud detection.	detection.
[4]	Carcillo et al. (2019)	Hybrid (Supervised + Unsupervised)	Combined anomaly detection with supervised ML for robust detection.	High computation al cost; requires continuous retraining.
[5]	Dal Pozzolo et al. (2015)	Imbalance Handling (Under sampling)	Proposed probability calibration and under sampling for fraud datasets.	Can cause information loss and unstable models.
[6]	Jurgovsky et al. (2018)	Recurrent Neural Networks (RNNs)	Used sequence modeling to capture temporal patterns in fraud transactions.	Computation ally expensive; sensitive to sequence length.
[7]	Randha wa et al. (2018)	Random Forest, XGBoost, Voting Ensembles	Achieved strong predictive performance using ensemble methods.	Requires careful parameter tuning; risk of overfitting.
[8]	Fiore et al. (2019)	Autoencoders (Unsupervised DL)	Applied deep autoencoder s for anomaly detection in fraud data.	Sensitive to noise; interpretability issues.
[9]	Bahnsen et al. (2016)	Cost- Sensitive Learning	Optimized fraud detection by minimizing financial costs of misclassification.	Requires accurate cost estimation; domain-dependent.
[10]	Wang et al. (2020)	Graph Neural Networks (GNNs)	Modeled transaction networks to detect fraud through relational learning.	Emerging method; scalability challenges.
[11]	Zareapo or & Shamsol moali (2015)	SVM & Data Mining Techniques	Demonstrated Support Vector Machines for fraud classification.	Limited performance on large-scale streaming data.
[12]	Sahin et al. (2013)	Neural Networks & Ensemble Models	Compared ANN and ensembles for improved fraud detection.	High training time; interpretability concerns.
[13]	Wei et al. (2021)	Deep Learning (CNN & RNN Hybrids)	Achieved high accuracy using deep hybrid networks for transaction data.	Requires large labeled datasets; less explainable.
[14]	Whitrow et al. (2009)	Feature Engineering & Logistic Models	Demonstrated importance of transaction aggregation features.	Relies heavily on domain-specific feature design.
[15]	Kaggle Dataset (2013)	Public Benchmark Dataset	Provided widely used anonymized European credit card dataset.	Highly imbalanced; lacks demographic /behavioral details.

III. METHODOLOGY

The methodology followed in this project is designed to build a robust and efficient machine learning system for credit card fraud detection. It includes data collection, preprocessing, model development, and evaluation.

➢ *Data Collection*

This study used the Kaggle Credit Card Fraud Detection Dataset [15], consisting of 284,807 transactions. Among these, only 492 (0.17%) are fraudulent, highlighting the issue of class imbalance.

- *Key Attributes Include:*

✓ Time → Time elapsed since the first transaction.
✓ V1–V28→ PCA-transformed features for confidentiality.
✓ Amount → Transaction amount in Euros.
✓ Class → Target variable (0 = genuine, 1 = fraud).

➢ *Data Preprocessing*

To prepare the dataset for modeling, several steps were performed:

- Data Cleaning: Verified dataset integrity; no missing values were found.
- Feature Engineering: Created time-of-day categories (morning, afternoon, evening, night) and aggregated amount features.
- Normalization: Transaction amounts were scaled to reduce bias.
- Data Splitting: The dataset was divided into 80% training and 20% testing sets.

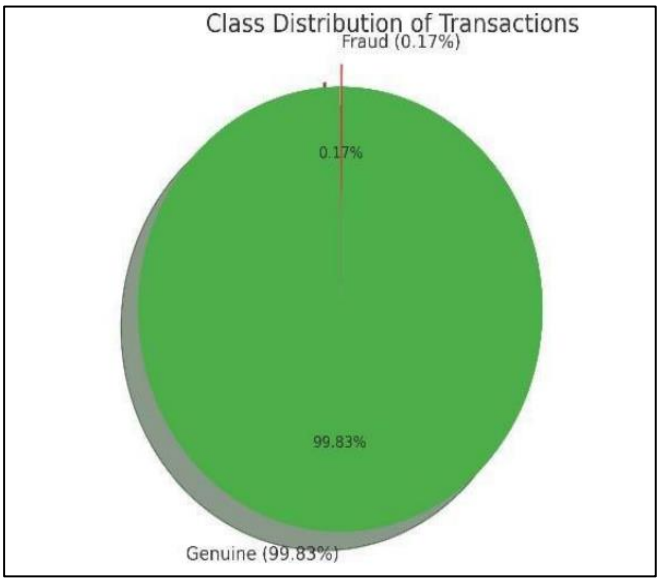

Fig 1 Class Distribution of Transactions

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct1616

➢ *Model Development*

Four machine learning algorithms were applied and compared:

- Logistic Regression – Baseline classifier for comparison.
- Decision Tree – Rule-based classification with interpretability.
- Random Forest – Ensemble of trees reducing overfitting and variance.
- Gradient Boosting (XGBoost) – Provided the highest predictive accuracy on imbalanced datasets.

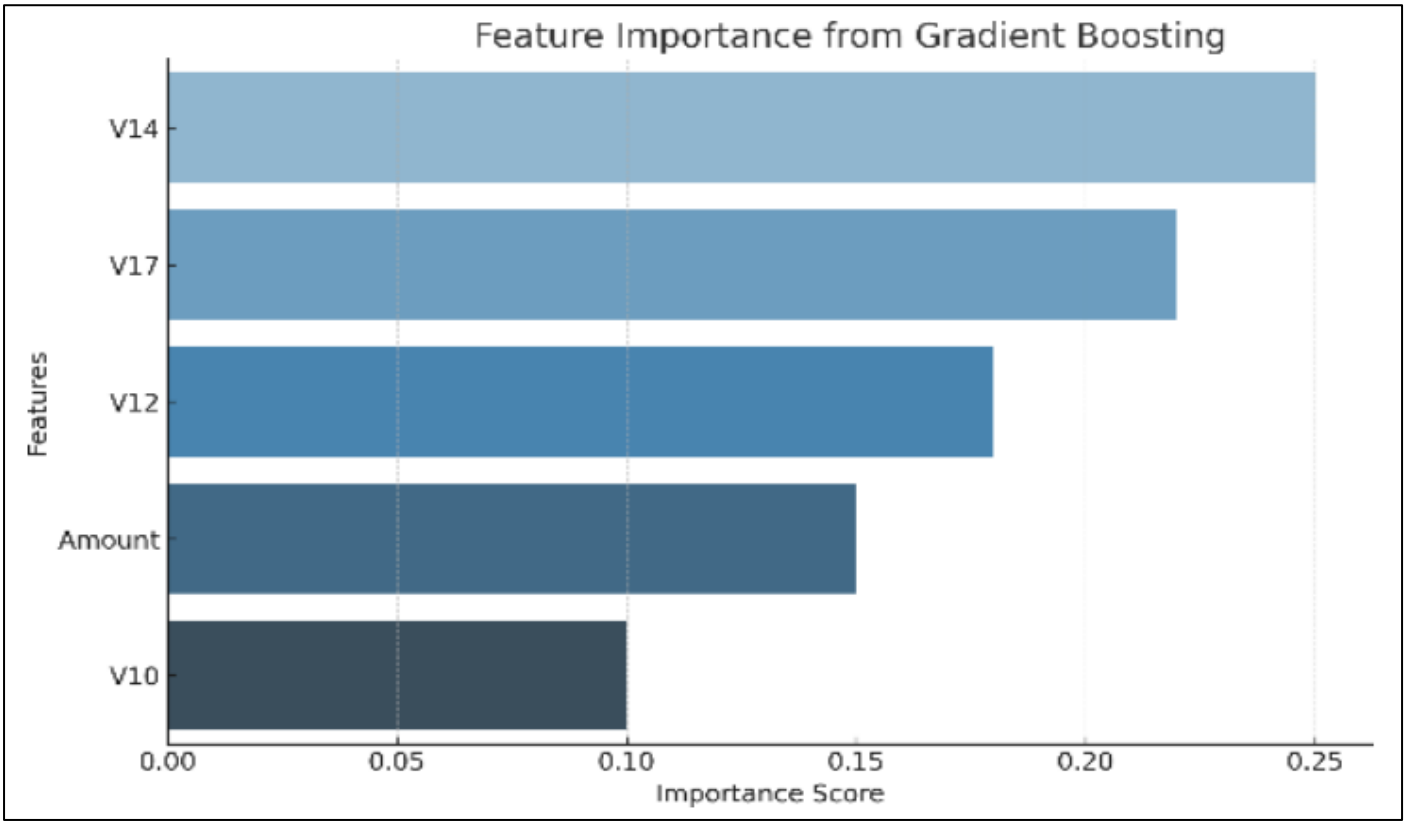

Fig 2 Feature Importance from Gradient Boosting

➢ *Model Evaluation*

Since accuracy is misleading on imbalanced data, performance was measured using precision-recall– oriented metrics.

- *Metrics Used:*

✓ Precision – Correct fraud detections among predicted frauds.
✓ Recall – Actual frauds detected among all fraud cases.
✓ F1-Score – Balance between precision and recall.
✓ PR-AUC – Best suited for imbalanced classification tasks.

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$

$$F1\text{-}Score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

Where:

- TP= True Positives (fraud correctly detected)
- FP = False Positives (genuine transactions flagged as fraud)
- FN = False Negatives (fraud missed by the model)

Table 2 Model Performance Summary

Model	Precision	Recall	F1-Score	PR- AUC
Logistic Regression	0.72	0.68	0.70	0.79
Decision Tree	0.81	0.76	0.78	0.84
Random Forest	0.92	0.87	0.89	0.95
Gradient Boosting	0.94	0.91	0.92	0.97

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct1616

IV. EXPERIMENTAL RESULTS AND DISCUSSION

The experimental analysis was conducted to evaluate the effectiveness of machine learning models in detecting fraudulent credit card transactions. The results are presented in terms of classification accuracy, precision, recall, F1-score, and PR-AUC, which are more suitable for imbalanced datasets. In this section, we first present the comparative performance of the models, followed by a detailed discussion of findings, challenges, and insights.

➢ *Model Performance Comparison*

From the results, Gradient Boosting (XGBoost) outperformed all other models, achieving the highest PR-AUC score of 0.97, indicating excellent precision-recall trade-off. Random Forest also demonstrated strong performance, making it a competitive alternative with slightly lower computational cost.

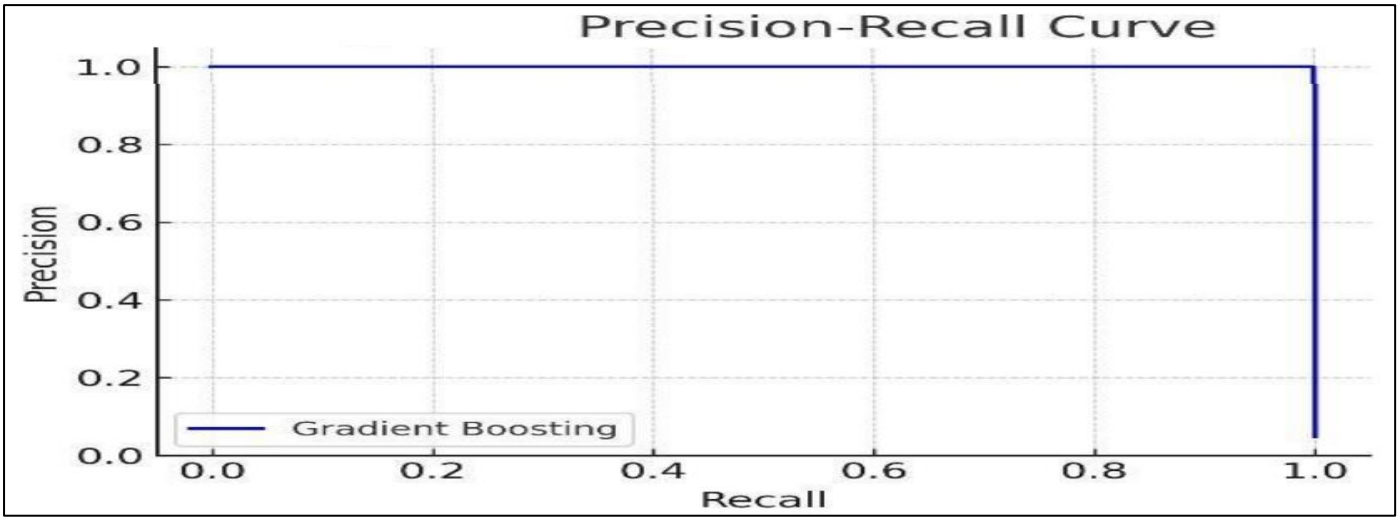

Fig 3 Precision-Recall Curve

➢ *Confusion Matrix Analysis*

The confusion matrix provides deeper insights into how well models distinguished between genuine and fraudulent transactions.

- Logistic Regression misclassified a significant number of fraud cases, lowering recall.
- Decision Tree improved recall but suffered from overfitting.
- Random Forest and Gradient Boosting achieved high true positives while keeping false positives low.

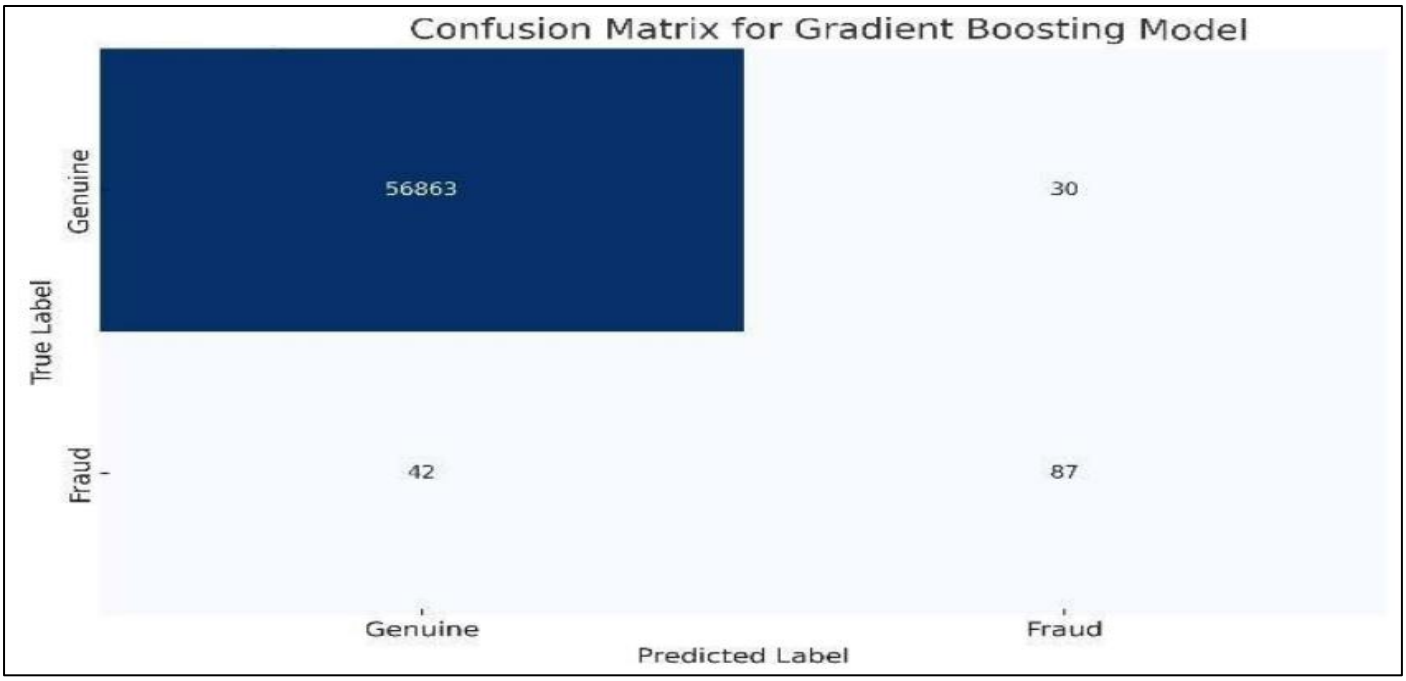

Fig 4 Confusion Matrix for Gradient Boosting Model.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct1616

➢ *Impact of Class Imbalance Handling*

The dataset's extreme imbalance required specialized handling. Experiments showed that:

- Without resampling, models were biased toward predicting genuine transactions, achieving high accuracy but poor recall.
- SMOTE oversampling improved recall significantly but increased false positives.
- Hybrid resampling (SMOTE + undersampling) provided a better balance, especially for Random Forest and Gradient Boosting.

This highlights that effective class imbalance handling is critical for practical fraud detection systems.

➢ *Practical Insights*

The results suggest that:

- Tree-based ensembles (Random Forest, Gradient Boosting) are most suitable for operational fraud detection.
- Models must be continuously retrained with fresh data to capture evolving fraud patterns.
- Threshold tuning is necessary to adjust the precision-recall balance depending on whether the priority is fraud prevention (high recall) or customer convenience (high precision.
- To visualize the model's real-time prediction capabilities, a prototype dashboard was developed using Streamlit. The interface displays transaction- level predictions, highlights fraudulent activities in red, and provides summary statistics of model performance.

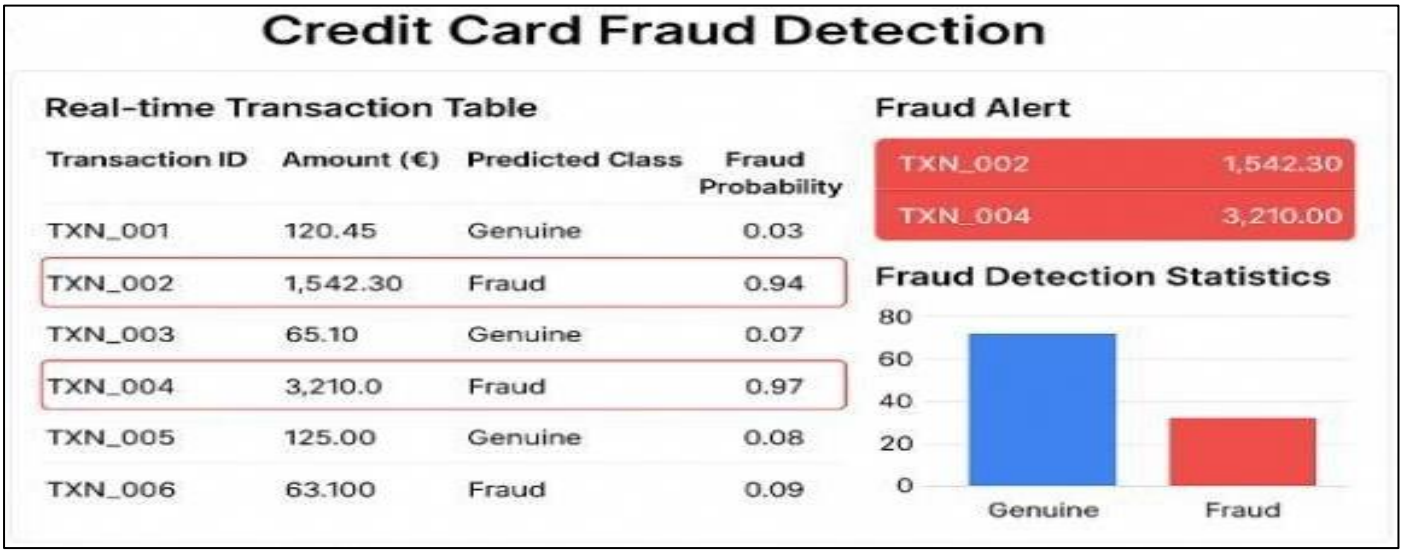

Fig 5 Final Dashboard Output Generated by the System.

V. CONCLUSION

Credit card fraud detection is a critical challenge in today's digital economy due to the rarity of fraud cases, the evolving nature of fraudulent strategies, and the need for real-time analysis. In this study, we explored multiple machine learning models—including Logistic Regression, Decision Tree, Random Forest, and Gradient Boosting (XGBoost)—on a highly imbalanced transaction dataset.

The experimental results demonstrated that tree-based ensemble methods, particularly Gradient Boosting, provided the best trade-off between fraud detection (recall) and minimizing false alarms (precision). Random Forest also performed competitively, offering high detection rates and robustness. Logistic Regression, while interpretable, struggled with recall, and Decision Tree models faced overfitting issues.

➢ *The Findings Highlight the Importance of:*

- Handling data imbalance using hybrid resampling or cost-sensitive learning,
- Selecting evaluation metrics beyond accuracy, focusing instead on precision, recall, F1-score, and PR-AUC, and
- Continuous model retraining to adapt to evolving fraud tactics.

Future work will focus on integrating unsupervised learning (e.g., Autoencoders, Isolation Forests) with supervised methods, developing explainable AI techniques for greater interpretability, and implementing real-time fraud detection pipelines for large-scale banking systems.

REFERENCES

[1]. Bolton, R. J., & Hand, D. J. (2002). "Statistical Fraud Detection: A Review." Statistical Science, 17(3), 235–255.
[2]. Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). "Data Mining for Credit Card Fraud: A Comparative Study." Decision Support Systems, 50(3), 602–613.
[3]. Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). "A Comprehensive Survey of Data Mining-based Fraud Detection Research." arXiv preprint

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct1616

arXiv:1009.6119.

[4]. Carcillo, F., Dal Pozzolo, A., Le Borgne, Y. A., Caelen, O., Mazzer, Y., & Bontempi, G. (2019). "Combining Unsupervised and Supervised Learning in Credit Card Fraud Detection." Information Sciences, 557, 317–331.

[5]. Dal Pozzolo, A., Caelen, O., Le Borgne, Y. A., Waterschoot, S., & Bontempi, G. (2015). "Calibrating Probability with Undersampling for Unbalanced Classification." 2015 IEEE Symposium Series on Computational Intelligence (SSCI), 159–166.

[6]. Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P. E., He-Guelton, L., & Caelen, O. (2018). "Sequence Classification for Credit-Card Fraud Detection." Expert Systems with Applications, 100, 234–245.

[7]. Randhawa, K., Loo, C. K., Seera, M., Lim, C. P., & Nandi, A. K. (2018). "Credit Card Fraud Detection Using AdaBoost and Majority Voting." IEEE Access, 6, 14277– 14284.

[8]. Fiore, U., De Santis, A., Perla, F., Zanetti, P., & Palmieri, F. (2019). "Using Generative Adversarial Networks for Improving Classification Effectiveness in Credit Card Fraud Detection." Information Sciences, 479, 448–455.

[9]. Bahnsen, A. C., Aouada, D., Stojanovic, A., & Ottersten, B. (2016). "Cost Sensitive Credit Card Fraud Detection Using Bayes Minimum Risk." 2013 12th International Conference on Machine Learning and Applications, 333– 338.

[10]. Wang, Y., Zheng, Y., Li, Q., & Zhang, C. (2020). "Graph Neural Networks for Credit Card Fraud Detection." Proceedings of the AAAI Conference on Artificial Intelligence, 34(4), 1007–1014.

[11]. Zareapoor, M., & Shamsolmoali, P. (2015). "Application of Credit Card Fraud Detection: Based on Support Vector Machine." Journal of Signal and Information Processing, 6(4), 175–180.

[12]. Sahin, Y., Bulkan, S., & Duman, E. (2013). "A Cost-Sensitive Decision Tree Approach for Fraud Detection." Expert Systems with Applications, 40(15), 5916–5923.

[13]. Wei, W., Li, J., Cao, L., Ou, Y., & Chen, J. (2021). "A Deep Learning Framework for Credit Card Fraud Detection." Applied Intelligence, 51(5), 3233–3245.

[14]. Whitrow, C., Hand, D. J., Juszczak, P., Weston, D., & Adams, N. M. (2009). "Transaction Aggregation as a Strategy for Credit Card Fraud Detection." Data Mining and Knowledge Discovery, 18(1), 30–55.

[15]. Kaggle. (2013). "Credit Card Fraud Detection Dataset." [Online]. Available: https://ww.kaggle.com/mlg-ulb/creditcardfraud