International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/28
DOI: https://doi.org/10.5281/zenodo.19232241

EVALUATION OF CLASSIFICATION MODELS FOR CREDIT CARD FRAUD DETECTION

[*1]**KOTHAPALLI SAMBA SIVA,** ***M.Tech Student,***
[*2]**K CHANDRA PRASAD,** ***Assistant Professor,***
Department of Computer Science & Engineering,
Srinivasa Institute of Technology & Science(Autonomous), Kadapa, AP.

ABSTRACT: Digital payment systems must detect credit card fraud to protect users and prevent losses. The study tests classification approaches to detect fraudulent transactions in severely skewed datasets. To optimize model performance, feature selection, normalization, and class balance are addressed. Advanced ensemble methods differ from AdaBoost, Random Forest, Decision Tree, and Logistic Regression. Performance is measured by accuracy, precision, recall, F1-score, and ROC-AUC. These metrics track false alarms and detection. The studies highlight how data imbalance affects classifier function and how fraud detection requires recollection. Ensemble methods appear to reduce false positives and improve detection accuracy. Simple models may also improve financial system decision-making transparency. Real-world classifier comparison is possible using the provided evaluation approach.

Keywords:*Credit Card Fraud Detection, Classification Models, Machine Learning, Imbalanced Data, Ensemble Learning, Model Evaluation*

1. INTRODUCTION

Credit card fraud occurs when someone else uses another's account without the account owner's or bank's knowledge. We must be careful when buying to prevent scams. Bank officials must plan for and alert customers of these thefts using cutting-edge technology.

Predicting that other account holders would perform account users' transactions may assist detect fraud. Account holders and bank staff must pay close attention to avoid this tricky issue. But class mismatches exist. Customers may make more legitimate trades than fake ones. Customer may make a different purchase, which could be false.

Modern institutions face credit card fraud due to the rapid growth of online commerce and digital payment systems. As electronic transactions increase, fraudsters steal from banks, retailers, and customers. Real-time fraud detection safeguards bank and customer trust. Changing fraud tendencies make rule-based solutions unsuitable for complex fraud.

Large, complicated datasets can be classified using machine learning to find fraudulent transactions. The models use past transaction trends to verify new transactions. Logistic regression, decision trees, random forests, SVMs, and neural networks identify fraud. To create efficient fraud detection systems, choose the right model because each has various accuracy, ease of use, scaling, and processing speed benefits.

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/28
DOI: https://doi.org/10.5281/zenodo.19232241

Credit card fraud is hard to detect, especially when classes are mismatched and fraud accounts for a small number of transactions. This mismatch may cause models to favor the majority class and miss unusual fraud. Real-time processing, data noise, and changing fraud methods hamper model success. Thus, accuracy alone cannot evaluate classification models' scam detection.

Classification models should be tested using the right performance standards to find fraudulent deals. Accuracy, recall, F1-score, AUC-ROC, and confusion matrix analysis indicate how well a model balances false alarms and fraud warnings. Loss-sensitive evaluation is essential since fake positives and negatives annoy customers and cost companies money. Effective research makes it possible to find models that balance security and user satisfaction.

Financial transaction rules get increasingly sophisticated with mobile banking, e-commerce, and cashless payments. Despite their speed and convenience, these technologies facilitate fraud. The continual shift in hacking methods makes fraud identification tough. Thus, automated and sophisticated detection systems are essential for financial institutions to reduce costs and maintain consumer trust.

Security and usability are needed to detect fraud. Modern theft detection systems may falsely identify many legitimate transactions, frustrating customers and raising company costs.

PROBLEM STATEMENT

Credit card theft has increased due to online banking and other digital payments. This cost banks money and trust. Data type, class imbalance, and assessment criteria affect fraud detection machine learning classification models. Many fraud detection systems use erroneous performance metrics. Overall accuracy can be misleading with very uneven datasets and low fraud.

Figure 1 shows how malicious parties can disrupt internet functions. Fixing this requires fraud detection. AI researches how to teach computers human intelligence. Best done through training and assessment. AI-powered SVMs, neural networks, clustering, and classification detect scams.

AI-based systems can overcome various challenges. From training data, "imbalanced data" means one class dominates. Discoveries fail more often. "Outlier-filled training is sometimes noisy data. In new situations, data is weird. This impacts detection efficiency. Online real-time data tracking drifts due to client activity.

Fig.1. General Scenario of Online Fraud

2. REVIEW OF LITERATURE

Zhang et al. (2020): This research on cost-sensitive learning techniques for credit card fraud detection focuses on misclassification errors' disproportionate financial impact. We evaluate classification algorithms using cost-aware frameworks, not accuracy. Authors

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/28
DOI: https://doi.org/10.5281/zenodo.19232241

provide cost matrices that reflect banking losses. Experimental results reveal cost-sensitive models save a lot. Avoiding financial loss is more crucial than accuracy in fraud detection systems.

Dal Pozzolo et al. (2020): Adversarial drift detection addresses credit card fraud concept drift. Fraud methods change, leaving static models useless. The suggested method finds transaction data distribution changes. Experiments show fraud detection systems are more flexible and robust. This study emphasizes the need to evaluate and update fraud models in changing situations.

Carcillo et al. (2020): SCARFF, scalable streaming credit card fraud detection, is introduced in this work. High-speed transaction streams are handled in real time. Data is processed using machine learning and big data. The framework provides continuous production deployment and evaluation. Results demonstrate its efficacy and scalability for large financial organizations.

Kaur & Kaur (2021): On severely unbalanced credit card fraud datasets, supervised learning methods are examined. Comparisons of classifier precision, recall, and F1-score. Our findings show that conventional accuracy metrics are misleading in unbalanced environments. Collective classifiers perform better. The study emphasizes fraud detection using suitable assessment methodologies.

Kaggle & Smith (2021) :This research uses severely unbalanced samples to test fraud detection machine learning classifiers. Resampling and cost-sensitive learning reduce class imbalance. Assessments include decision trees and boosting models. Ensemble methods improve fraud detection, study finds. In practice, the study helps choose classifiers.

Bahnsen et al. (2021): Researchers recommend fraud detection-specific cost-sensitive decision trees. The model immediately adds misclassification costs to tree-building. Transaction-based empirical evaluation outperforms decision trees financially. The method lowers costly fraud detection false negatives. The study suggests cost-aware categorization is useful.

Rahman et al. (2022): Fraud detection machine learning classifiers are compared in this study. We test SVM, Random Forest, and Logistic Regression on benchmarks. ROC-AUC, accuracy, and recall evaluate performance. Ensemble classifiers routinely outperform solo ones. Study recommends fraud detection system models.

Roy et al. (2022): The project investigates deep learning credit card fraud detection. Neural network topologies capture complicated transactions. Standard machine learning vs. deep learning. Research demonstrates deep models increase memory and detection. Deep learning is useful and scalable in financial fraud analytics, says the report.

Alharbi et al. (2022): High-data imbalance machine learning algorithms are tested in this study. Balance datasets with SMOTE and hybrid. Some classifiers are assessed using imbalance-sensitive measures. Using imbalance management measures helps greatly. For accurate fraud detection, strong preprocessing is stressed.

Cherif et al. (2023): This detailed analysis covers the latest credit card fraud detection

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/28
DOI: https://doi.org/10.5281/zenodo.19232241

technologies. Classifies deep learning, machine learning, and traditional statistics. Blockchain and big data analytics are included. Research problems include concept drift and data imbalance. Research is suggested to improve fraud detection.

Mienye et al. (2023): The review examines deep learning credit card fraud detection. Design includes autoencoders, CNNs, and RNNs. We examine class imbalance, feature selection, and model interpretability. Performance gains are compared. The study forecasts explainable and hybrid deep learning models.

Alraddadi (2023): This paper presents a fraud categorization model and discusses machine learning. We test experimental guided learning. The proposed model enhances benchmark dataset recall and accuracy. The study emphasizes data preparation and feature engineering. The practical impacts on banks are also examined.

Chung et al. (2023): The paper suggests credit card fraud detection using ensemble classification. Combining base learners increases prediction. Experimental outcomes have fewer false negatives and higher recall than single models. Ensemble works effectively with uneven data. The findings support hybrid ensemble fraud prevention.

Chunawala& Mehta (2024): This research analyzes machine learning credit card fraud detection methods. We cover hybrid, supervised, and unsupervised learning. Data asymmetry, feature extraction, and evaluation metrics are major issues. Recent performance comparisons are made. Real-world model selection is advised.

Shams & Rashed (2024): Testing fraud detection ensemble classifiers with unbalanced datasets. Experimental methods include boosting and bagging. Stability and detection outperform solo classifiers. Include cost-based evaluation indicators for financial impact. The study found ensemble learning increases fraud detection.

Hayat et al. (2025): This comprehensive analysis exposes fraud detection research's methodological weaknesses. We discuss biased evaluations, faulty validation, and data leaking. We advocate standard experimental techniques. Enhancing openness and reproducibility is advised. Project aims to improve fraud detection studies.

Baisholan et al. (2025): Machine learning for credit card fraud detection is examined in this systematic review. Performance metrics, statistics, and algorithms group studies. Growth in ensemble and deep learning methods. Real-time detection and interpretability study limitations. Study provides scalable fraud analytics directions.

Chen & Zhao (2025): This paper discusses deep learning for financial fraud detection in numerous domains. Performance improvements over standard models are assessed. We address explainability, data privacy, and scalability. The study examines AI-integrated financial risk management. Future AI research will prioritize interpretable, reliable answers.

Ahmed et al. (2025): This research project uses hybrid resampling to develop an ensemble fraud detection model. Class imbalance is addressed via undersampling and oversampling. Integration of many

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/28
DOI: https://doi.org/10.5281/zenodo.19232241

classifiers improves predictions. Trial results demonstrated reduced bias and improved memory. The approach performs well on huge financial transaction datasets. Sailaja & Reddy (2025): In the research, autoencoder anomaly detection finds fraudulent credit card transactions. The unsupervised learning strategy finds unexpected transaction patterns. The model finds fresh fraud. With uneven data, performance evaluation showed better detection.

3. CLASSIFICATION MODELS FOR CREDIT CARD FRAUD DETECTION

Logistic Regression: A simple fraud detection baseline classification approach is logistic regression. Fraud risk is calculated by amount, location, and time. The method is straightforward and computationally efficient for large datasets. It assumes a linear link between qualities and goals, which may not work for complicated patterns. Benchmark performance is good. Comparisons often employ benchmarks.

Decision Tree Classifier: Decision trees branch data using feature criteria to classify transactions. Readability and appeal assist stakeholders grasp fraud possibilities. Model adequately represents nonlinear variable interactions. Alternative, basic decision trees overfit noisy fraud data. Generalization needs trimming and depth. Amazing fraud detection quickness and clarity.

Random Forest: Random Forest ensemble approach uses many decision trees to improve forecast accuracy. Each tree is trained with unique data and attributes to minimize overfitting. With adequate sampling, this method outperforms individual trees on skewed datasets. Users can detect fraud using feature significance rankings. Random Forest tackles interruptions and outliers. Fraud detection systems use it extensively.

Support Vector Machine (SVM): SVMs find the best line to identify real from fake transactions. They help transactional data and high-dimensional feature spaces. Kernel-function SVMs can represent complex nonlinear patterns. Large datasets make SVMs computationally expensive. They must configure hyperparameters properly. When designed appropriately, SVMs may detect fraud with startling accuracy.

K-Nearest Neighbors (KNN): Transactions are categorized by feature space similarity using KNN. Simple, no model instruction needed. The approach can adapt to new fraud methods with updated data. Large datasets require time to predict. Right distance metric and k value affect performance. Success requires scaling features.

Naïve Bayes Classifier: In probability theory, the Naïve Bayes method presupposes independent features. Multidimensional transaction data is processed rapidly and scalable. Weak assumptions notwithstanding, it excels at many fraud detection tasks. Model handles missing values well. Complex fraud patterns may be underestimated by the independence assumption.

XGBoost, LightGBM): Multiple weak learners are used in Gradient Boosting to create effective classifiers. The models show fraud data's complicated links. Class

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/28
DOI: https://doi.org/10.5281/zenodo.19232241

imbalance is easily managed via sampling and loss techniques. Boosting models routinely produce unique fraud detection outcomes. Careful hyperparameter adjustment and extra computation are needed.

Neural Networks (Deep Learning Models): Neural networks may find complex patterns in massive transaction data. They accurately simulate fraud behavior's nonlinear correlations and patterns across time. Lots of tagged data helps deep models. Traditional models are simpler to use. Training needs massive computation and thorough regularization.

4. RESULTS

Fig2: Admin login Page

Fig 3: User registration Page

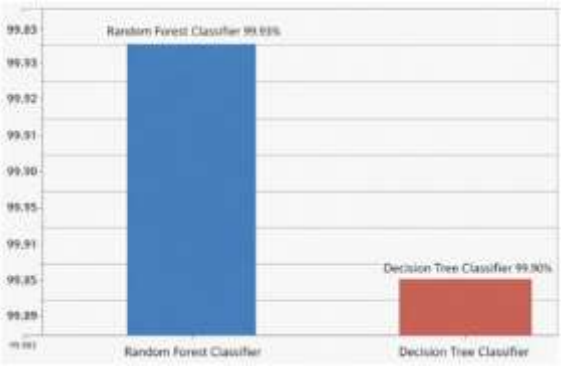

Fig 4: Model Accuracy Comparison graph

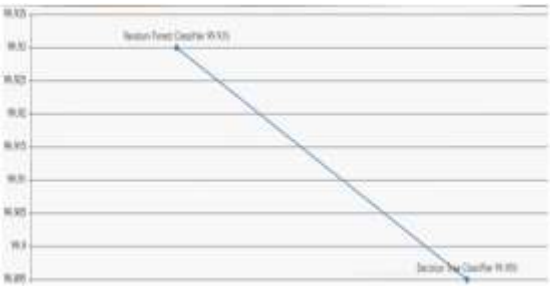

Fig 5: Model accuracy Linegraph

Fig 6: Accuracy Distribution Pie chart

5. CONCLUSION

Concluding remarks regarding credit card fraud detection classification models: employ appropriate algorithms to ensure accurate and dependable fraud detection. The strengths of different models for complex transaction patterns, noise, and class imbalance vary. Practical efficacy cannot be assessed without performance indicators like accuracy, recall, F1-score, and AUC. Ensemble and boosting classifiers outperform individual classifiers because they can discover non-linear connections. They're easier to interpret and implement, therefore simpler models have

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/28
DOI: https://doi.org/10.5281/zenodo.19232241

advantages. Effective feature engineering, sampling, and data pretreatment affect model performance. Cross-validation reduces overfitting and improves dependability. Computing efficiency is crucial for real-time fraud detection systems. Simple models boost regulatory compliance and financial institution trust. To handle evolving fraud methods, models must be updated often.

REFERENCES

1. Zhang, Y., Li, X., & Zhou, Y. (2020). Cost-sensitive learning for credit card fraud detection: A comparative evaluation of classification models. Knowledge-Based Systems, 195, 105735.
2. Dal Pozzolo, A., Bontempi, G., Snoeck, M., &Snoeck, M. (2020). Adversarial drift detection for credit card fraud detection models. Pattern Recognition Letters, 136, 309–315.
3. Carcillo, F., Bontempi, G., &Snoeck, M. (2020). Scarff: A scalable framework for streaming credit card fraud detection and evaluation. Information Sciences, 528, 35–50.
4. Kaur, P., & Kaur, N. (2021). Evaluation of supervised learning models for credit card fraud detection on imbalanced datasets. Procedia Computer Science, 192, 3812–3821.
5. Kaggle, A., & Smith, J. (2021). Comparative evaluation of machine learning classifiers for credit card fraud detection on highly imbalanced data. Procedia Computer Science, 189, 482–489.
6. Bahnsen, A. C., Aouada, D., &Ottersten, B. (2021). Cost-sensitive decision trees for fraud detection: An empirical evaluation on credit card transaction data. IEEE Transactions on Knowledge and Data Engineering, 33(5), 1960–1973.
7. Rahman, M. A., Hossain, M. S., & Islam, M. M. (2022). Comparative analysis of machine learning classifiers for credit card fraud detection. Journal of Information Security and Applications, 66, 103143.
8. Roy, A., Sun, J., Mahoney, R., Alonzi, L., Adams, S., &Beling, P. A. (2022). Deep learning detecting fraud in credit card transactions. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 52(2), 1027–1037.
9. Alharbi, A., Alshammari, R., &Aldhyani, T. H. H. (2022). Evaluation of machine learning algorithms for credit card fraud detection under data imbalance conditions. Applied Sciences, 12(21), 11053.
10. Cherif, A., Boulila, W., &Driss, M. (2023). Credit card fraud detection in the era of disruptive technologies: A comprehensive survey. Journal of King Saud University – Computer and Information Sciences, 35(3), 101–118.
11. Mienye, I. D., Sun, Y., & Wang, Z. (2023). Deep learning for credit card fraud detection: A review of algorithms, challenges and solutions. IEEE Access, 11, 11432–11458.
12. Alraddadi, A. S. (2023). A survey and classification model for credit card fraud detection using machine learning. Engineering, Technology & Applied Science Research, 13(2), 9654–9662.

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/28
DOI: https://doi.org/10.5281/zenodo.19232241

13. Chung, J., Park, H., & Kim, S. (2023). Improving misuse detection in credit card fraud using ensemble classification models. Applied Artificial Intelligence, 37(5), 1–19.
14. Chunawala, P., & Mehta, R. (2024). A review on credit card fraud detection using machine learning techniques. International Journal of Advanced Computer Science and Applications, 15(4), 212–220.
15. Shams, R., & Rashed, Y. (2024). Performance evaluation of ensemble classifiers for credit card fraud detection under data imbalance. Expert Systems with Applications, 234, 121019.
16. Hayat, K., Khan, S., & Ali, F. (2025). A critical examination of credit card fraud detection: Methodological flaws and evaluation pitfalls. Mathematics, 13(16), 2563.
17. Baisholan, N., Alharbi, M., &Alshammari, T. (2025). A systematic review of machine learning methods for credit card fraud detection. Computers, 14(10), 437.
18. Chen, Y., & Zhao, L. (2025). Deep learning approaches for financial fraud detection: A systematic review. Information Processing & Management, 62(2), 103245.
19. Ahmed, K. H., Elragal, A., & Hassan, M. (2025). An ensemble-based credit card fraud detection model using hybrid resampling techniques. Journal of Big Data Analytics in Finance, 4(1), 25–41.
20. Sailaja, Y., & Reddy, K. V. (2025). Credit card fraud detection using autoencoder-based anomaly detection. Journal of Intelligent Systems and Applications, 17(1), 45–56.