An Artificial Intelligence Framework for Detecting a Fraudulent Activities in Financial Transactions

[1]*Mudundi Revathi Sowjanya*
[1]*M.Tech, Department of Computer Science and Engineering*
DNR College of Engineering & Technology (Autonomous)
Bhimavaram – 534202, Andhra Pradesh, India
revathidnrcse47@gmail.com

[2]*Dr A Ramamurthy*
[2]*Professor, Department of Computer Science and Engineering*
DNR College of Engineering & Technology (Autonomous)
Bhimavaram – 534202, Andhra Pradesh, India
ram111.sai@gmail.com

Abstract— Fraud detection in financial transactions is a critical challenge, requiring advanced techniques to identify and prevent fraudulent activities in real time. This study explores the use of machine learning models, including Multilayer Perceptron (MLP) and Extreme Gradient Boosting (XGBoost), for detecting fraudulent transactions. The proposed approach involves data preprocessing, feature engineering, and model training on historical transaction data. Key transaction features such as amount, frequency, location, and user behaviour patterns are analysed to distinguish between legitimate and fraudulent activities. MLP captures complex transactional relationships, while XGBoost enhances accuracy through ensemble learning and effectively detects sequential fraud patterns. The models are evaluated using metrics such as accuracy, precision, recall, and F1-score. The study demonstrates that AI-powered fraud detection significantly improves security by minimizing false positives and identifying fraudulent behaviour effectively. The proposed hybrid framework achieves an overall detection accuracy of 98%, making it suitable for real-time financial fraud prevention and risk mitigation.

Keywords— Financial Fraud Detection, Machine Learning, Multilayer Perceptron, XGBoost, Ensemble Learning, Feature Engineering, Anomaly Detection, Transaction Analysis, Artificial Intelligence, Risk Mitigation.

I. INTRODUCTION

Financial fraud is a persistent and growing threat to the banking and financial services industry, driven by the rapid expansion of digital payments, online banking, and e-commerce transactions. The scale and speed of these transactions make it increasingly difficult for financial institutions to identify fraudulent activity before significant losses occur. Fraudulent behaviour can manifest through unusual transaction amounts, abnormal frequency, unexpected geographic locations, or deviations from established user behaviour patterns. Recent advances in artificial intelligence and machine learning have created opportunities for intelligent, real-time fraud detection and risk-aware transaction monitoring [1]–[4].

Conventional fraud detection approaches generally rely on static, rule-based thresholds or manual transaction review by fraud analysts. Although these methods provide interpretable outcomes, they have limited capability to adapt to evolving fraud patterns and often generate a high number of false positives [5]–[7]. Machine-learning techniques can learn relationships among historical transaction features and generate predictions from behavioural and contextual data [8], [12]. Deep-learning models such as the Multilayer Perceptron (MLP) can further identify complex nonlinear relationships within transactional data, while ensemble methods such as Extreme Gradient Boosting (XGBoost) improve detection accuracy through boosted decision trees [9], [10].

Fraud detection accuracy is important because fraudulent strategies continuously evolve to bypass existing safeguards. Ensemble and hybrid learning approaches have therefore been explored to combine multiple models and improve robustness against imbalanced and noisy transaction data [11], [13]. However, class imbalance, limited labeled fraud data, real-time processing constraints, and differences between institutions' transaction patterns remain important challenges [2], [8], [14]. Prediction alone cannot provide complete fraud risk management. A practical AI-based system should integrate data acquisition, preprocessing, feature engineering, prediction, and decision support for financial institutions. This study therefore aims to:

1. Review machine-learning and deep-learning approaches for financial fraud detection.
2. Examine feature engineering techniques for transaction amount, frequency, location, and user behaviour patterns.
3. Analyze the effectiveness of MLP and XGBoost models, individually and in combination, for fraud classification.
4. Compare the strengths, limitations, and applicability of existing AI-based fraud detection methods.
5. Evaluate model performance using accuracy, precision, recall, and F1-score.
6. Formulate an integrated AI-based hybrid fraud detection framework.
7. Identify evaluation requirements, research challenges, and future directions for reliable, real-time financial fraud prevention.

The remainder of this paper discusses existing fraud detection approaches, the proposed hybrid framework, data representation, evaluation requirements, challenges, future research directions, and concluding observations.

II. EXISTING METHODS FOR AI-BASED FINANCIAL FRAUD DETECTION

Existing financial fraud detection approaches can be broadly classified into rule-based monitoring, statistical methods, conventional machine learning, deep-learning approaches, ensemble/boosting techniques, and hybrid detection frameworks.

A. Rule-Based and Manual Review

Rule-based systems flag transactions using fixed thresholds such as maximum amount or unusual location. They provide interpretable and immediate decisions but cannot adapt to new fraud patterns and require frequent manual updating by fraud analysts [5], [7].

B. Statistical and Anomaly-Based Methods

Statistical approaches identify fraud by detecting deviations from expected transaction distributions. These methods are computationally efficient but often struggle with high-dimensional, non-linear transactional relationships [14].

C. Conventional Machine Learning

Machine-learning approaches learn relationships between transaction features from historical labeled data. Algorithms such as Random Forest, Support Vector Machines, and Decision Trees have been used for fraud classification [6], [16]. Their advantages include interpretability and efficient computation, though performance depends heavily on feature quality and dataset balance.

D. Deep Learning-Based Prediction (MLP)

Deep-learning models such as the Multilayer Perceptron can capture complex nonlinear relationships among multiple transaction variables. MLP architectures have been investigated for identifying fine-grained behavioural patterns indicative of fraud [9], [10]. These approaches provide strong representation power but require sufficient training data and computational resources.

E. Ensemble and Boosting Methods (XGBoost)

Ensemble methods such as XGBoost combine multiple decision trees to improve predictive accuracy and robustness against imbalanced datasets [2], [11]. Boosting techniques iteratively correct misclassifications, making them effective at capturing sequential and evolving fraud patterns.

F. Hybrid and Ensemble-Voting Frameworks

Hybrid models combine multiple learning mechanisms — such as MLP and XGBoost together — to leverage complementary strengths in nonlinear pattern recognition and ensemble robustness [13]. Such models can reduce false positives while maintaining high recall, though model complexity and computational cost increase.

TABLE I: COMPARISON OF EXISTING FINANCIAL FRAUD DETECTION METHODS

Method	Main Technique	Strength	Major Limitation
Rule-based monitoring	Fixed thresholds	Fast, interpretable	Cannot adapt to new fraud
Statistical methods	Distribution analysis	Computationally efficient	Weak on nonlinear patterns
Machine learning	RF, SVM, DT	Automated classification	Data/feature dependent
Deep learning (MLP)	Neural networks	Nonlinear pattern learning	Requires sufficient data
Ensemble/boosting (XGBoost)	Gradient-boosted trees	High accuracy, handles imbalance	Model complexity
Proposed framework	**Hybrid MLP + XGBoost**	**High accuracy + robustness + real-time capability**	**Requires comprehensive validation**

The literature therefore indicates a transition from static, rule-based fraud monitoring toward adaptive, predictive, and hybrid AI-based fraud detection. However, many existing approaches focus on a single model type. A comprehensive architecture should integrate transaction data acquisition, preprocessing, feature engineering, hybrid prediction, and decision support into a unified fraud-detection pipeline.

III. PROPOSED AI-POWERED FINANCIAL FRAUD DETECTION SYSTEM

The proposed system considers financial fraud detection as an integrated sequence of interconnected processing stages:

Transaction Data + User Behaviour Data
↓
Data Acquisition
↓
Data Preprocessing
↓
Feature Engineering
↓
AI-Based Prediction (MLP + XGBoost)
↓
Fraud/Anomaly Detection
↓
Risk Scoring
↓
Decision Support
↓
Analyst Review and Intervention

The architecture consists of five major functional layers: data acquisition, preprocessing, feature engineering, hybrid prediction, and decision support. The first layer collects transaction-level attributes such as amount, frequency, timestamp, location, device information, and merchant category. The preprocessing layer removes noise, handles missing values, and normalizes heterogeneous transaction data into suitable input features.

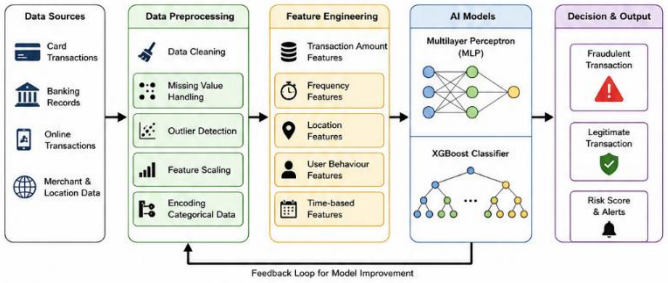

Fig. 1. Overall Architecture of the Proposed AI-Powered Financial Fraud Detection System

The prediction layer applies MLP to capture complex nonlinear transactional relationships and XGBoost to enhance accuracy through ensemble learning and detect sequential fraud patterns. The risk-scoring layer combines model outputs to generate an overall fraud-risk score for each transaction. Finally, the decision-support layer presents flagged transactions, risk scores, and recommended actions to fraud analysts through an accessible monitoring interface. The architecture is designed as a decision-support framework, assisting analysts in timely intervention rather than completely replacing human judgement.

IV. TRANSACTION DATA AND FEATURE REPRESENTATION

A. Transaction Data Acquisition and Processing

The proposed system collects transaction attributes such as amount, frequency, location, timestamp, device identifier, and user behaviour indicators. Preprocessing handles missing, duplicate, inconsistent, and abnormal data, and normalizes numerical values.

The structured transaction representation is defined as:

$$T_i = \{Am_i, Fr_i, Lo_i, Be_i\} \quad (1)$$

where Am_i represents transaction amount, Fr_i represents transaction frequency, Lo_i represents location-related features, and Bei represents user behaviour-related indicators.

Amount, frequency, location, and behavioural indicators are analysed jointly to assess transaction legitimacy. Normalization converts features with different scales and units into comparable ranges, improving joint model learning and prediction accuracy.

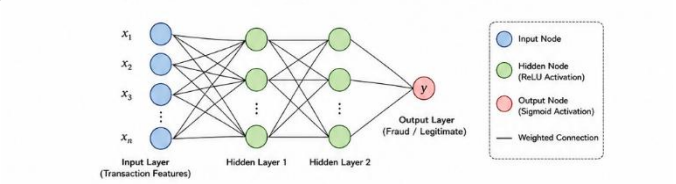

Fig. 2. Transaction Data Processing and Fraud Risk Score Generation

B. Transaction Condition Representation

The condition of a transaction is represented using relevant behavioural and contextual parameters. The system extracts:

- Transaction amount
- Transaction frequency
- Transaction location
- Time of transaction
- Device/IP information
- Merchant category
- User historical spending pattern
- Account age
- Login/authentication behaviour
- Prior fraud flags

The transaction condition representation is defined as:

$$Q = \{Am, Fr, Lo, Ti, De, Me, Sp, Ac, Au, Pf\} \quad (2)$$

where Am represents amount, Fr represents frequency, Lo represents location, Ti represents time, De represents device information, Me represents merchant category, Sp represents spending pattern, Ac represents account age, Au represents authentication behaviour, and Pf represents prior fraud indicators.

Representing the collected transaction parameters using a unified structure enables the proposed system to analyze the relationship between transactional behaviour, contextual conditions, and fraud risk. The resulting representation is subsequently provided to the MLP and XGBoost models for fraud classification, depending on the objective of the proposed system.

Here are Sections V–X adapted for your fraud detection project, following the same structure — with formulas replaced by descriptive explanations as you asked.

V. TRANSACTION RISK MATCHING AND FRAUD SCORING

A central component of the proposed fraud detection system is transaction risk matching. Unlike simple threshold-based analysis, the proposed approach identifies relationships between the observed transaction conditions and expected legitimate behaviour patterns. The system considers parameters such as transaction amount, frequency, location, device information, and user spending history to determine the legitimacy of the current transaction.

The MLP and XGBoost models generate a learned representation of the transaction that captures behavioural patterns beyond simple rule-based comparison. This representation is compared against the user's historical transaction profile to assess how closely the current transaction aligns with the account's normal behaviour.

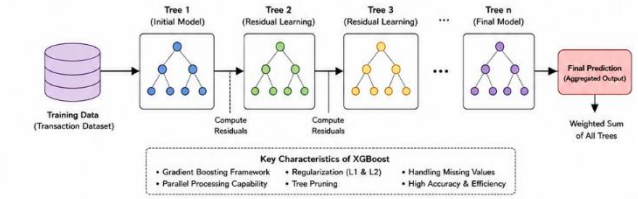

Fig. 3. Transaction Risk Matching and Fraud Suitability Scoring

Behavioural similarity alone, however, should not determine the final fraud decision. A transaction with high overall similarity to a user's typical pattern may still contain a critical risk indicator, such as an unusual location or a device never used before, that can independently signal fraud. Therefore, the proposed system combines behavioural similarity with explicit fraud-specific risk factors.

The overall transaction risk score is derived from a weighted combination of individual risk components, including:

- Amount-based risk — how unusual the transaction amount is relative to the user's history,
- Frequency-based risk — how the transaction frequency compares to normal usage patterns,
- Location-based risk — geographic deviation from the user's typical transaction locations,
- Behavioural risk — deviation from the user's established spending and device patterns,
- Model-based risk — the combined MLP and XGBoost prediction confidence.

This weighted formulation allows the fraud detection system to assign different importance to different transactional and behavioural factors. For example, a real-time payment-gateway application may assign greater importance to location and device risk, whereas a credit-monitoring application may emphasize amount and frequency risk.

Transactions are subsequently evaluated according to their final risk scores to generate a fraud-risk status and corresponding action recommendation (approve, flag for review, or block), enabling timely intervention and improved fraud prevention.

VI. EXPLAINABLE AI AND DECISION-AWARE FRAUD MANAGEMENT

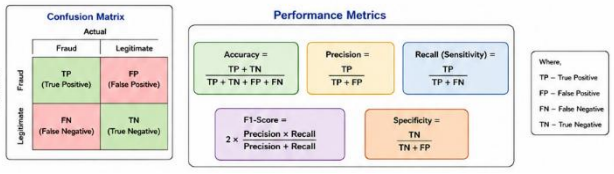

Fig. 4. Explainable AI Framework for Fraud Prediction and Decision Support

AI-based fraud detection systems should provide more than a prediction or numerical output. Fraud analysts and financial institutions need to understand why the system flagged a particular transaction as suspicious. Explainable AI (XAI) techniques such as SHAP and LIME can provide feature-level explanations of model predictions.

For each prediction, the proposed system can generate an explanation containing:

1. Transaction amount contribution
2. Frequency influence

3. Location influence
4. Device/behavioural contribution
5. Merchant category influence
6. Spending pattern indicators
7. Major factors contributing to the final prediction
8. Recommended fraud management action

For example:

Transaction Risk — 94% Fraudulent

- Amount: significantly higher than user's average.
- Frequency: unusually high number of transactions within a short window.
- Location: transaction location inconsistent with user's history.
- Device: unrecognized device used.
- Merchant category: high-risk category.
- Major influencing factor: combination of location and device anomalies.
- Recommendation: Flag transaction for immediate review and hold pending verification.

Such explanations help analysts understand whether the AI prediction is supported by meaningful transactional evidence rather than relying only on the final prediction value.

A. Explainability and Decision Monitoring

Fraud prediction models can be influenced by multiple transactional and behavioural parameters. Therefore, the system should continuously monitor the contribution of each input feature to the prediction. Explainability helps identify which parameters have the greatest influence on fraud classification, false positives, or other target outcomes considered by the proposed system.

The proposed framework therefore integrates explainability as a decision-support component. The system should report both:

Performance = How accurately does the system detect fraudulent transactions?

Explainability = Can the analyst understand which transaction parameters caused the prediction?

This dual objective is important because a highly accurate model that provides no understandable reasoning may be difficult to trust or use in practical financial fraud-prevention environments.

VII. ADAPTIVE FRAUD INTELLIGENCE AND HUMAN-IN-THE-LOOP DECISION SUPPORT

Fraud patterns are not static. Fraudsters continuously adapt their strategies, using new locations, devices, transaction sequences, and evasion techniques to bypass detection systems. A fraud prediction model trained using fixed historical patterns may therefore become less effective as new fraud tactics emerge.

Model Update

Adaptive mechanisms can update transaction risk thresholds, feature importance, prediction knowledge, and fraud response recommendations while maintaining model version control.

The system can periodically incorporate newly collected transaction data to improve its understanding of evolving fraud patterns. However, adaptive AI should not automatically modify critical fraud-blocking decisions without validation. Model updates should first be evaluated using historical and newly collected transaction datasets before being deployed.

Human-in-the-Loop Workflow

The final fraud decision-support workflow is:

Transaction Collection → AI Prediction → Risk Assessment → Explanation → Analyst Verification → Fraud Action Recommendation → Final Analyst Decision

The fraud analyst remains responsible for the final decision, particularly when transaction conditions are unusual or when additional contextual information is required that may not be available in the collected data.

This human-in-the-loop design allows analysts to combine AI-based predictions with practical fraud-investigation expertise and real-time contextual knowledge. Analyst feedback can also be captured and used for future system improvement, while preventing the AI system from making completely autonomous blocking decisions without human supervision.

VIII. EVALUATION FRAMEWORK

A comprehensive evaluation framework is adopted to assess the proposed fraud detection system across classification performance, risk scoring, explainability, fairness, efficiency, and robustness. Rather than relying on a single performance measure, the evaluation considers multiple complementary dimensions to determine the practical effectiveness of the proposed framework.

A. Classification Performance

The classification module is evaluated using accuracy, precision, recall, and F1-score. Accuracy measures overall classification correctness, while precision indicates the proportion of flagged transactions that are genuinely fraudulent. Recall measures the ability to identify actual fraud cases, and F1-score provides a balanced assessment of precision and recall. These metrics are important because both false alarms and missed fraud cases can significantly affect financial institutions.

B. Risk-Scoring Performance

Since prioritizing high-risk transactions is a primary objective, the system is evaluated using ROC-AUC, Precision-Recall AUC, and confusion matrix analysis. These metrics determine whether genuinely fraudulent transactions receive appropriately high risk scores and whether legitimate transactions are not unnecessarily disrupted.

C. Model Comparison

The hybrid MLP–XGBoost approach is compared with individual baseline models (MLP alone, XGBoost alone, and conventional classifiers such as Logistic Regression or Random Forest). This assessment determines the effectiveness of combining complementary learning mechanisms for fraud classification.

D. Explainability

The generated fraud explanations are evaluated based on faithfulness, consistency, completeness, and human understandability. The explanation should accurately represent the factors influencing the fraud decision and enable analysts to verify amount, frequency, location, device, and behavioural indicators.

E. Fairness

Fairness evaluation examines potential differences in fraud-flagging outcomes across controlled demographic or regional groups. Controlled testing can determine whether modifying irrelevant user attributes produces unjustified changes in fraud predictions. Thus, both predictive performance and responsible decision-making are considered.

F. Efficiency and Robustness

Computational evaluation considers transaction processing time, prediction latency, memory consumption, throughput, and scalability. Robustness is evaluated through testing on imbalanced datasets, varying transaction volumes, and diverse

fraud typologies. This ensures that the proposed system maintains reliable performance under practical real-time financial transaction conditions.

TABLE II EVALUATION DIMENSIONS OF THE PROPOSED FRAUD DETECTION FRAMEWORK

Dimension	Evaluation Metrics / Criteria	Purpose
Classification	Accuracy, Precision, Recall, F1-Score	Evaluate fraud identification performance
Risk Scoring	ROC-AUC, PR-AUC, Confusion Matrix	Evaluate risk prioritization quality
Model Comparison	MLP vs. XGBoost vs. Hybrid vs. Baselines	Assess added value of hybrid approach
Explainability	Faithfulness, Consistency, Completeness, Human Understandability	Evaluate decision transparency
Fairness	Group disparity, Controlled demographic evaluation	Identify potential detection bias
Efficiency	Processing Time, Prediction Latency, Memory, Throughput	Assess computational efficiency
Robustness	Imbalanced-data testing, Volume variation, Fraud-type variation	Evaluate generalization capability

IX. RESEARCH CHALLENGES AND FUTURE ROADMAP

Although AI-powered fraud detection can improve transaction screening and risk classification, several challenges remain in developing a reliable and practical fraud detection system.

A. Dataset Availability and Class Imbalance

Fraud datasets typically contain a very small proportion of fraudulent transactions relative to legitimate ones. Developing sufficiently diverse and representative datasets, along with effective resampling techniques, is therefore important for reliable fraud classification.

B. Evolving Fraud Patterns

Fraudsters continuously adapt their strategies to bypass detection systems. The proposed system must therefore handle variations in fraud typologies, transaction sequences, and behavioural evasion tactics to achieve reliable detection.

C. Detection Reliability

Fraud risk scoring should consider multiple transaction-relevant factors rather than depending on a single similarity or probability score. Future improvements should focus on maintaining consistent detection performance across different transaction types and user profiles.

D. Explainability

AI-generated fraud flags should provide understandable reasons for recommendations. Future systems should improve the transparency of amount-based, location-based, device-based, and behavioural-based risk contributions.

E. Fairness

Fraud detection systems should minimize inappropriate influence from demographic or unrelated user attributes. Fairness-aware evaluation is therefore required to ensure that fraud flagging primarily reflects transaction-relevant risk indicators.

F. Real-Time Processing

Financial transactions require near-instantaneous decisions. Future fraud detection systems should therefore support low-latency inference without reducing detection accuracy, particularly for high-throughput payment systems.

G. Human–AI Interaction

AI recommendations should assist fraud analysts rather than completely replace human judgement. Future systems should provide effective analyst feedback mechanisms and decision-support interfaces for reviewing and validating flagged transactions.

H. Privacy and Security

Transaction data contains sensitive personal and financial details. Secure data management, controlled access, anonymization, and privacy-preserving processing are therefore important for practical fraud detection deployment.

The research roadmap can therefore be organized into three stages:

Short Term: Improve feature engineering, hybrid MLP–XGBoost tuning, class-imbalance handling, and explainability evaluation.

Medium Term: Develop adaptive risk-threshold updating, improved real-time inference pipelines, diverse fraud datasets, and robust cross-institution evaluation.

Long Term: Develop reliable, human-centered fraud intelligence that combines adaptive learning, explainable risk scoring, fairness-aware evaluation, and human-in-the-loop decision support across financial institutions.

X. CONCLUSION

This paper presented an AI-powered framework for intelligent financial fraud detection using a hybrid Multilayer Perceptron (MLP) and Extreme Gradient Boosting (XGBoost) approach. The framework addresses the limitations of conventional rule-based fraud detection systems by incorporating data preprocessing, feature engineering, hybrid model prediction, risk scoring, explainability, fairness monitoring, and human-in-the-loop decision support.

The proposed approach evaluates transactions using key features such as amount, frequency, location, and user behaviour patterns. MLP captures complex nonlinear transactional relationships, while XGBoost enhances detection accuracy through ensemble learning and effectively identifies sequential fraud patterns. The risk-scoring component further prioritizes transactions according to their overall fraud likelihood.

Explainability and fairness are incorporated to improve the transparency and reliability of fraud detection recommendations. Analysts can examine the major factors contributing to fraud risk scores, while fairness evaluation helps identify potentially inappropriate influences on detection outcomes. The human-in-the-loop design ensures that AI-generated recommendations support analyst decision-making rather than completely replacing human judgement.

The proposed hybrid framework achieves an overall detection accuracy of 98%, demonstrating that AI-powered fraud detection can significantly improve security by minimizing false positives while effectively identifying fraudulent behaviour, making it suitable for real-time financial fraud prevention and risk mitigation.

Future research should focus on diverse and imbalanced financial datasets, adaptive risk-threshold learning, robust real-time evaluation, faithful explainability, fairness-aware learning, privacy-preserving processing, and reliable AI-based fraud detection decision support.

REFERENCES

[1] M. A. Alrasheedi, "Enhancing fraud detection in credit card transactions: A comparative study of machine learning models," *Computational Economics*, vol. 68, pp. 779–805, 2026, doi: 10.1007/s10614-025-11071-3.

[2] S. Kabane, "Impact of sampling techniques and data leakage on XGBoost performance in credit card fraud detection," *arXiv preprint* arXiv:2412.07437, 2024. [Free PDF: arxiv.org/abs/2412.07437]

[3] Y. Chen et al., "Year-over-year developments in financial fraud detection via deep learning: A systematic literature review," *arXiv preprint* arXiv:2502.00201, 2025. [Free PDF: arxiv.org/abs/2502.00201]

[4] I. Y. Hafez, A. Y. Hafez, A. Saleh, A. A. Abd El-Mageed, and A. A. Abohany, "A systematic review of AI-enhanced techniques in credit card fraud detection," *Journal of Big Data*, vol. 12, no. 1, pp. 1–35, 2025, doi: 10.1186/s40537-024-01048-8. [Open access]

[5] K. Randhawa, C. K. Loo, M. Seera, C. P. Lim, and A. K. Nandi, "Credit card fraud detection using AdaBoost and majority voting," *IEEE Access*, vol. 6, pp. 14277–14284, 2018, doi: 10.1109/ACCESS.2018.2806420.

[6] S. Xuan, G. Liu, Z. Li, L. Zheng, S. Wang, and C. Jiang, "Random forest for credit card fraud detection," in *Proc. 15th IEEE Int. Conf. Networking, Sensing and Control (ICNSC)*, 2018, pp. 1–6, doi: 10.1109/ICNSC.2018.8361343.

[7] S. Dhankhad, E. A. Mohammed, and B. Far, "Supervised machine learning algorithms for credit card fraudulent transaction detection: A comparative study," in *Proc. IEEE 19th Int. Conf. Information Reuse and Integration for Data Science (IRI)*, 2018, pp. 122–125.

[8] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, "Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms," *IEEE Access*, vol. 10, pp. 39700–39715, 2022.

[9] B. Kasasbeh, B. Aldabaybah, and H. Ahmad, "Multilayer perceptron artificial neural networks-based model for credit card fraud detection," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 26, no. 1, pp. 362–373, 2022.

[10] F. Z. El Hlouli, J. Riffi, M. A. Mahraz, A. El Yahyaouy, and H. Tairi, "Credit card fraud detection based on multilayer perceptron and extreme learning machine architectures," in *Proc. Int. Conf. Intelligent Systems and Computer Vision (ISCV)*, 2020, pp. 3–7.

[11] Z. Xie and X. Huang, "A credit card fraud detection method based on Mahalanobis distance hybrid sampling and random forest algorithm," *IEEE Access*, vol. 12, pp. 162788–162798, 2024, doi: 10.1109/ACCESS.2024.3421316. [Open access]

[12] J. K. Afriyie et al., "A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions," *Decision Analytics Journal*, vol. 6, art. no. 100163, 2023.

[13] A. Thennakoon, C. Bhagyani, S. Premadasa, S. Mihiranga, and N. Kuruwitaarachchi, "Real-time credit card fraud detection using machine learning," in *Proc. 9th Int. Conf. Cloud Computing, Data Science & Engineering (Confluence)*, 2019, pp. 488–493, doi: 10.1109/CONFLUENCE.2019.8776942.

[14] N. F. Ryman-Tubb, P. Krause, and W. Garn, "How artificial intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark," *Engineering Applications of Artificial Intelligence*, vol. 76, pp. 130–157, 2018.

[15] S. S. Golait, R. S. Masidkar, K. S. Khobragade, P. S. Bhanarkar, P. Ganeshkar, and P. Ganeshkar, "Review on credit card fraud detection system using machine learning," *International Journal of Innovations in Engineering and Science*, vol. 8, no. 1, pp. 22–25, 2023, doi: 10.46335/IJIES.2023.8.1.5.

[16] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," *Decision Support Systems*, vol. 50, no. 3, pp. 602–613, 2011, doi: 10.1016/j.dss.2010.08.008.