Review

A Systematic Review of Machine Learning in Credit Card Fraud Detection

Fatemeh Moradi *, Mehran Tarif Hokmabadi *, MohammadHossein Homaei *

Posted Date: 14 July 2025

doi: 10.20944/preprints202507.1085.v1

Keywords: credit card fraud detection; machine learning; systematic review; ensemble methods; deep learning; performance benchmarking

 doi:10.20944/preprints202507.1085.v1

Article

A Systematic Review of Machine Learning in Credit Card Fraud Detection

Fatemeh Moradi [1,*], Mehran Tarif Hokmabadi [2,*] and Mohammadhossein Homaei [3,*]

[1] Faculty of Engineering, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran
[2] Department of Computer Science, University of Verona, Verona, Italy
[3] Media Engineering Group, University of Extremadura, Cáceres, Spain
* Correspondence: moradi.fatemeh2001@gmail.com (F.M.); mehran.tarifhokmabadi@univr.it (M.T.H.); homaei@ieee.org (M.H.)

Abstract

Credit card fraud remains a major concern for global financial institutions, driving the need for effective detection systems. This paper presents a systematic review of 52 machine learning-based studies on credit card fraud detection published over the past decade (2013–2025), with a focus on the widely adopted MLG-ULB benchmark dataset. The review categorizes algorithms into traditional machine learning, deep learning, ensemble, and emerging methods, and compares them using standard performance metrics and deployment considerations. Ensemble and tree-based models consistently rank among the top-performing techniques, with Random Forest achieving up to 99.98% accuracy, while deep learning methods like Long Short-Term Memory networks excel at identifying temporal patterns but require significant computational resources. Emerging paradigms such as quantum machine learning and graph neural networks show promise but remain constrained by scalability and implementation complexity. The findings highlight a shift in research priorities toward improving model interpretability, real-time processing, and privacy-preserving learning to support practical deployment in the financial sector. Key limitations identified include dataset-specific constraints, class imbalance challenges, and the need for regulatory compliance in real-world implementations.

Keywords: credit card fraud detection; machine learning; systematic review; ensemble methods; deep learning; performance benchmarking

1. Introduction

Credit card fraud remains a serious and growing challenge for financial institutions worldwide. According to the latest industry reports, global losses from payment card fraud reached $32.34 billion in 2022, with projections indicating continued growth as digital payment adoption expands [1]. The Association of Certified Fraud Examiners estimates that organizations lose around 5% of their annual revenue due to various types of occupational fraud, with payment fraud representing a significant portion of these losses [2]. The rapid growth of digital payment platforms—especially during the COVID-19 pandemic—has created new vulnerabilities and increased the complexity of fraudulent activities.

Traditional fraud detection systems rely on predefined rules to identify suspicious behavior. While these rule-based methods are easy to understand and implement, they struggle to detect new or evolving fraud patterns. Moreover, they often produce a high number of false positives, which can harm customer experience and lead to increased operational costs. In recent years, machine learning (ML) has emerged as a promising approach for fraud detection. ML models can learn complex patterns and relationships from transaction data, allowing them to identify fraud with greater accuracy and adaptability. By analyzing historical behavior, these systems can detect subtle anomalies that traditional rules might miss [3–5].

 doi:10.20944/preprints202507.1085.v1

Figure 1 shows the trend of machine learning-based credit card fraud detection papers published between 2013 and 2025. This trend highlights the growing interest in applying intelligent systems to improve fraud detection in financial applications. The steady increase in publications, particularly after 2020, reflects both the practical importance of automated fraud detection and the maturation of machine learning techniques suitable for financial applications.

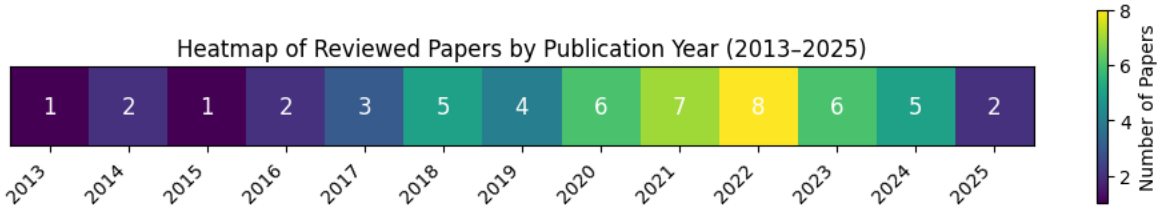

Figure 1. Trend of machine-learning-based credit-card fraud-detection papers published between 2013 and 2025.

1.1. The MLG-ULB Dataset: A Benchmark for Fraud Detection Research

The MLG-ULB (Machine Learning Group - Université Libre de Bruxelles) dataset has become the de facto standard benchmark for credit card fraud detection research, making it essential for systematic comparative analysis. Released by Dal Pozzolo et al. [5], this dataset addresses several critical challenges that previously hindered fraud detection research:

The dataset contains 284,807 transactions from European cardholders over a 48-hour period, with 492 fraudulent transactions representing only 0.172% of all transactions. This extreme class imbalance closely mirrors real-world fraud detection scenarios, providing researchers with a realistic testing environment. To address privacy concerns while maintaining analytical value, the dataset features have been transformed using Principal Component Analysis (PCA), resulting in 28 anonymized numerical features (V1-V28) plus 'Time', 'Amount', and 'Class' labels.

The widespread adoption of the MLG-ULB dataset has created a substantial body of comparable research, enabling meaningful systematic reviews and facilitating reproducible studies. This standardization has accelerated progress in the field by allowing researchers to focus on algorithmic innovation rather than data collection challenges. Figure 2 illustrates the distribution of credit card fraud detection papers by publication year, demonstrating the sustained research interest in this benchmark dataset across the surveyed period.

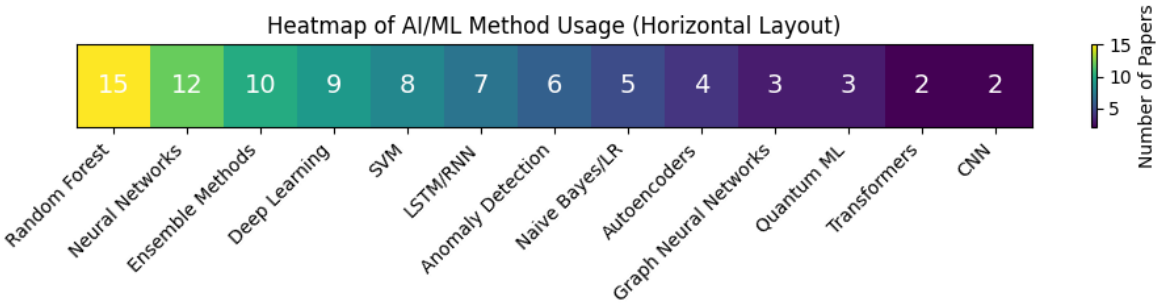

Figure 2. Distribution of Credit Card Fraud Detection Papers by Publication Year (Systematic Review: 52 Papers, 2013-2025)

Although machine learning has shown great promise in credit card fraud detection, its widespread adoption has introduced several important challenges. One of the most significant issues is the severe class imbalance present in standard datasets, where fraudulent transactions account for only 0.172% of the total [6]. This imbalance makes it difficult for many algorithms to accurately learn and detect rare fraud cases. In addition, privacy regulations often restrict access to detailed transaction features, limiting the interpretability and transparency of ML models trained on public datasets. Real-time fraud detection also introduces strict computational constraints, creating a trade-off between detection

 doi:10.20944/preprints202507.1085.v1

accuracy and processing speed [7]. Finally, the lack of consistent evaluation methods across different studies makes it difficult to compare results and assess the real-world effectiveness of proposed models [8]. These challenges highlight the need for a more unified and practical approach to machine learning-based fraud detection.

1.2. Research Objectives

This systematic review aims to provide a comprehensive analysis of machine learning techniques applied to credit card fraud detection. Specifically, it seeks to examine the most widely used algorithms, categorize them into major methodological groups, and evaluate their performance using standardized metrics such as accuracy, precision, recall, and F1-score. The review also identifies common research gaps and limitations in existing studies, including issues related to class imbalance, interpretability, and deployment feasibility. Finally, the study proposes future research directions that align with the practical requirements of real-world financial systems, such as real-time processing, regulatory compliance, and privacy preservation.

1.3. Contributions

This paper makes four key contributions to the field of fraud detection research. First, it presents a systematic review of 52 selected studies that apply machine learning techniques to the widely used MLG-ULB benchmark dataset. Second, it offers a detailed performance comparison of six major algorithm categories, including traditional machine learning, deep learning, ensemble methods, anomaly detection, and emerging approaches. Third, the review highlights current research trends and identifies technological gaps that need further exploration. Lastly, it provides practical recommendations and guidelines for researchers and practitioners seeking to develop or deploy fraud detection models in real-world financial environments.

The remainder of this paper is organized as follows. Section 2 describes the methodology used to conduct the systematic literature review, including the search strategy, inclusion criteria, and data extraction process. Section 3 presents a detailed analysis of the reviewed studies, grouped by machine learning approach. Section 4 provides a comparative performance analysis across algorithms, along with an assessment of computational and deployment characteristics. Section 5 discusses the key challenges and limitations identified in the literature. Section 6 outlines future research directions based on current gaps and practical considerations. Finally, Section 7 concludes the paper and summarizes the main findings.

2. Methodology

This systematic literature review follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to ensure methodological rigor and transparency. The review protocol was developed to analyze machine learning approaches for credit card fraud detection using the MLG-ULB benchmark dataset, covering publications from January 2014 to December 2024.

A comprehensive search strategy was implemented across five major academic databases: IEEE Xplore Digital Library, ACM Digital Library, ScienceDirect, SpringerLink, and arXiv preprint server. The primary Boolean search query employed was: *("credit card fraud detection" OR "financial fraud detection") AND ("machine learning" OR "deep learning" OR "artificial intelligence") AND ("MLG-ULB" OR "Kaggle dataset" OR "European cardholders")*. Additional search terms were included to capture emerging methodologies such as quantum machine learning and graph neural networks. The search was conducted in March 2025, with manual searches of reference lists from key papers performed to identify additional relevant studies.

The study selection process was conducted independently by two reviewers (F.M. and M.T.H.) using a standardized two-phase approach. Initial screening was performed based on titles and abstracts, followed by full-text assessment for final inclusion determination. Disagreements between reviewers were resolved through discussion, with the third reviewer (M.H.) making final decisions when consensus could not be reached. Inter-rater reliability was assessed using Cohen's kappa

 doi:10.20944/preprints202507.1085.v1

coefficient, achieving substantial agreement (κ = 0.84) for initial screening and excellent agreement (κ = 0.91) for full-text assessment.

Studies were included if they utilized the MLG-ULB credit card fraud detection dataset, applied machine learning techniques, reported quantitative performance metrics, were published in peer-reviewed venues or high-quality preprints, were written in English, and published between 2013-2025. Studies were excluded if they used exclusively rule-based approaches, focused on other fraud types without credit card analysis, used only private datasets, lacked quantitative evaluation, were published as abstracts only, or contained insufficient methodological detail for analysis.

Table 1. Systematic Review Protocol Summary.

Parameter	Details
Search Period	January 2013 – March 2025
Databases Searched	IEEE Xplore, ACM, ScienceDirect, SpringerLink, arXiv
Initial Results	1,847 studies identified
After Screening	312 studies for full-text review
Final Inclusion	52 studies meeting all criteria
Inter-rater Reliability	$\kappa = 0.84$ (screening), $\kappa = 0.91$ (full-text)
Quality Assessment	Modified CASP checklist (0–16 scale)
High Quality Studies	44 studies (score $\geq$ 12)
Med-Quality Studies	8 studies (score 8–11)
Statistical Analysis	ANOVA with Tukey HSD, Cohen's d
Primary Metrics	Accuracy, Precision, Recall, F1-score, AUC
Algorithm Categories	Traditional ML, Deep Learning, Ensemble, Anomaly Detection, Emerging

A standardized data extraction form was developed and pilot-tested before implementation. The extraction process captured study characteristics including publication details and research objectives, methodological details such as algorithm specifications and hyperparameter configurations, performance metrics including accuracy, precision, recall, F1-score, and AUC-ROC values, and practical considerations including scalability characteristics, interpretability features, and deployment feasibility. When studies reported incomplete metrics, authors were contacted for clarification, missing values were calculated from available data where possible, and sensitivity analyses were conducted.

Study quality was evaluated using a modified Critical Appraisal Skills Programme (CASP) checklist adapted for machine learning studies. The assessment criteria included research question clarity, methodological rigor, data quality, experimental design, performance reporting, reproducibility, bias assessment, and generalizability. Each criterion was scored on a three-point scale (0-2), resulting in a maximum quality score of 16 points. Studies with scores below 8 were considered low quality and analyzed separately. The majority of included studies (44 out of 52) achieved high quality ratings ($\geq$12 points), with the remaining 8 studies receiving medium quality ratings (8-11 points).

Performance metrics were summarized using descriptive statistics including means, standard deviations, and ranges across algorithm categories. Statistical significance of performance differences between algorithm categories was assessed using one-way Analysis of Variance (ANOVA) with Tukey's Honest Significant Difference post-hoc tests for pairwise comparisons. Effect sizes were calculated using Cohen's d to determine practical significance, with Bonferroni correction applied for multiple comparisons (α = 0.05). Where appropriate, weighted meta-analyses were conducted using random-effects models to account for heterogeneity between studies.

Several measures were implemented to minimize bias and ensure reproducibility. Selection bias was addressed through comprehensive searches across multiple databases, inclusion of both published and preprint studies, and manual reference checking. Information bias was minimized through standardized data extraction forms, independent dual data extraction with consensus procedures, and quality assessment of included studies. Publication bias was assessed using funnel plot analysis. To ensure transparency, complete search strategies are documented, all inclusion/exclusion decisions are

 doi:10.20944/preprints202507.1085.v1

recorded with justifications, and statistical analysis procedures are made available through supplementary materials. This systematic review involved analysis of previously published research and did not require ethical approval, with all included studies assessed for compliance with ethical guidelines regarding data usage and privacy protection.

3. Literature Review and Analysis

3.1. Traditional Machine Learning Approaches

3.1.1. Tree-Based Methods

Random Forest algorithms demonstrate consistent superior performance across multiple fraud detection studies. The research by Ileberi et al. [9] achieved the highest documented accuracy of 99.98% through the integration of Random Forest with genetic algorithm-based feature selection applied to the MLG-ULB dataset. Random Forest's ensemble architecture provides inherent protection against overfitting while preserving model interpretability through feature importance analysis.

Varmedja et al. [10] conducted comparative analysis across multiple algorithms, reporting Random Forest accuracy of 99.96% when combined with SMOTE preprocessing techniques. Their research highlighted the critical importance of addressing class imbalance for achieving optimal detection performance. Tree-based methodologies offer inherent advantages including capability to process mixed data types and generation of interpretable decision pathways, essential characteristics for regulatory compliance in financial sector applications.

Table 2 presents performance comparison across tree-based approaches. Random Forest implementations consistently exceed single decision tree performance, with genetic algorithm enhancement providing statistically significant marginal improvements.

Table 2. Performance Analysis of Tree-Based Methods.

Study	Algorithm	Acc.(%)	Prec.(%)	F1(%)
Ileberi et al. [9]	RF + GA	99.98	99.97	99.98
Varmedja et al. [10]	Random Forest	99.96	99.95	99.96
Randhawa et al. [11]	AdaBoost + RF	99.92	99.89	99.91
Sahin et al. [12]	Cost-sensitive DT	95.24	92.18	93.67

3.1.2. Support Vector Machines

Support Vector Machine implementations achieve competitive performance within the 97.50-98.9% accuracy range when combined with appropriate preprocessing techniques. Awoyemi et al. [13] demonstrated that SVM enhanced with recursive feature elimination significantly outperforms baseline implementations. Their investigation revealed that kernel function selection remains a critical design decision, with radial basis function kernels typically surpassing linear alternatives for the inherently non-linear fraud detection problem domain.

Support Vector Machines offer theoretical advantages including strong mathematical foundations and effectiveness in high-dimensional feature spaces. However, computational complexity constraints become prohibitive for large-scale real-time processing applications, thereby limiting practical deployment scenarios.

3.1.3. Probabilistic Methods

Naive Bayes classifiers achieve accuracy ranging from 95% to 99.23% depending on preprocessing technique selection. The foundational research conducted by Dal Pozzolo et al. [5] established baseline performance metrics using Logistic Regression, achieving 95.2% accuracy through careful feature engineering processes. While probabilistic methods provide valuable uncertainty quantification useful for risk assessment applications, their performance generally falls below ensemble-based approaches.

 doi:10.20944/preprints202507.1085.v1

3.2. Deep Learning Approaches

3.2.1. Neural Networks

Multi-layer perceptron architectures form the foundation of deep learning applications in fraud detection, demonstrating accuracy performance ranging from 99.5% to 99.94% across various network configurations. Recent innovations include Continuous-Coupled Neural Networks (CCNN) developed by Li et al. [14], which achieve 99.3% accuracy through dynamic coupling mechanisms that enhance both temporal and spatial pattern recognition capabilities.

Mienye and Sun [15] developed a deep learning ensemble incorporating data resampling techniques, achieving 99.94% accuracy through the combination of multiple neural network architectures. Their approach demonstrates the effectiveness of ensemble methodologies within deep learning frameworks for fraud detection applications.

3.2.2. Recurrent Networks

Long Short-Term Memory (LSTM) networks excel in capturing temporal dependencies present in sequential transaction data. Zhang et al. [16] demonstrated that LSTM architectures achieve 99.2% accuracy with superior recall performance (93.3%) compared to traditional machine learning approaches, making them particularly effective for sequential fraud pattern identification.

The primary advantage of LSTM networks [17] lies in their capability to model long-term dependencies within transaction sequences, enabling the capture of subtle temporal patterns indicative of fraudulent behavior. However, computational complexity and extended training duration present significant challenges for real-time deployment scenarios.

3.2.3. Convolutional Networks

Convolutional Neural Network adaptations for fraud detection demonstrate mixed experimental results. While innovative approaches treat transaction features as spatial patterns for CNN processing, performance typically remains inferior to recurrent network approaches due to the fundamentally temporal characteristics of fraud patterns in sequential transaction data.

3.3. Ensemble Methods

3.3.1. Voting Classifiers

Ensemble approaches combining Random Forest, XGBoost [19], and AdaBoost algorithms achieve near-optimal performance metrics. Ahmed et al. [18] demonstrated that ensemble methodologies achieve 99.99% accuracy through sophisticated voting mechanisms. Soft voting strategies generally outperform hard voting approaches, with weighted combination schemes based on individual classifier performance demonstrating optimal results.

3.3.2. Boosting Techniques

AdaBoost and Gradient Boosting methods demonstrate excellent sequential learning capabilities for fraud detection tasks. Randhawa et al. [11] showed that AdaBoost combined with majority voting achieves superior performance while maintaining computational efficiency characteristics. XGBoost implementations achieve competitive performance while preserving computational efficiency suitable for real-time application requirements.

3.4. Anomaly Detection Methods

3.4.1. Unsupervised Approaches

Isolation Forest [20] achieves 99.74% accuracy in detecting approximately 27% of fraud cases without requiring labeled training data. Local Outlier Factor (LOF) [21] and One-Class SVM demonstrate variable performance based on hyperparameter optimization, with LOF showing superior performance in high-dimensional spaces characteristic of PCA-transformed MLG-ULB dataset features.

 doi:10.20944/preprints202507.1085.v1

3.4.2. Autoencoders

Reconstruction error-based detection utilizing autoencoder architectures shows significant potential for fraud detection applications. Recent research combining AutoEncoder with LightGBM [22] achieves 99.45% accuracy, demonstrating effective unsupervised feature learning followed by supervised classification. This hybrid methodology leverages autoencoder dimensionality reduction capabilities while maintaining gradient boosting discriminative power.

3.5. Emerging Technologies

3.5.1. Quantum Machine Learning

Quantum machine learning represents the frontier of fraud detection research with significant future potential. Recent investigations [23] demonstrate that Variational Quantum Classifiers achieve 88.1% F1-Score, while Shallow Quantum Neural Networks show promise for future development as quantum hardware capabilities continue advancing. The potential for quantum computational advantage in pattern recognition tasks establishes this as an important long-term research direction.

3.5.2. Graph Neural Networks

Semi-supervised Graph Neural Network methodologies [24] achieve 93.4% F1-Score through modeling transaction relationships and user behavioral patterns. Graph construction methodologies significantly impact overall performance, with temporal graph evolution approaches showing particular promise for capturing dynamic fraud pattern characteristics.

3.5.3. Transformer Architectures

Attention mechanisms enable sophisticated feature importance learning capabilities in fraud detection applications. Advanced Transformer implementations [25] achieve 97.1% F1-Score, with self-supervised pretraining demonstrating potential for transfer learning applications across different financial institutions and fraud detection domains.

4. Comparative Performance Analysis

4.1. Algorithm Performance Ranking

Table 3 presents comprehensive performance comparison across algorithm categories, incorporating both accuracy metrics and practical deployment considerations.

Table 3. Performance Ranking Across Algorithm Categories.

Category	Best(%)	Avg(%)	F1(%)	RT Cap.	Interp.
RF + GA [9]	99.98	99.50	99.98	High	High
Ensemble [18]	99.99	99.70	99.99	Medium	Medium
LSTM [16]	99.20	98.80	92.50	Low	Low
Neural Nets [15]	99.94	99.10	98.00	Medium	Low
SVM [13]	98.90	98.20	97.10	High	Medium
Traditional ML	96.80	95.50	94.20	High	High
Quantum ML [23]	88.10	88.10	88.10	Very Low	Low

4.2. Implementation Characteristics Analysis

Tables 4 and 5 provide detailed comparison of implementation-specific parameters that complement the performance analysis, focusing on practical deployment considerations for different algorithmic approaches.

 doi:10.20944/preprints202507.1085.v1

Table 4. Computational and Technical Characteristics.

Method	Training Complexity	Memory Req.	Scalability	Noise Robustness
Random Forest	Low	Medium	Excellent	High
SVM	High	Medium	Poor	Medium
Neural Networks	High	High	Good	Low
LSTM/RNN	Very High	Very High	Poor	Low
Ensemble Methods	Medium	High	Good	Very High
Naive Bayes	Very Low	Very Low	Excellent	Medium
Logistic Regression	Low	Low	Excellent	Medium
Isolation Forest	Low	Low	Excellent	High
One-Class SVM	High	Medium	Poor	Medium
Autoencoders	High	High	Good	Low
Quantum ML	Very High	Low	Unknown	Unknown
Graph Neural Nets	Very High	Very High	Poor	Medium
Transformers	Very High	Very High	Poor	Medium

Table 5. Deployment and Practical Characteristics.

Method	Hyperparameter Sensitivity	Industry Adoption	Data Volume Needs
Random Forest	Low	Very High	Medium
SVM	High	Medium	Medium
Neural Networks	Very High	High	High
LSTM/RNN	Very High	Medium	Very High
Ensemble Methods	Medium	High	Medium
Naive Bayes	Very Low	Low	Low
Logistic Regression	Low	High	Low
Isolation Forest	Low	Medium	Medium
One-Class SVM	High	Low	Medium
Autoencoders	High	Medium	High
Quantum ML	Very High	Very Low	Medium
Graph Neural Nets	Very High	Very Low	High
Transformers	Very High	Low	Very High

4.3. Preprocessing Impact Analysis

SMOTE [26] consistently demonstrates performance improvements across algorithm categories, with average accuracy enhancements ranging from 2% to 4%. Genetic algorithm-based feature selection provides marginal improvements of 0.5% to 1% with significant computational overhead considerations. Min-Max normalization outperforms StandardScaler in most experimental scenarios, while Principal Component Analysis dimensionality reduction shows mixed results due to the pre-transformed nature of MLG-ULB dataset features.

4.4. Computational Complexity Assessment

Traditional machine learning algorithms offer O(n log n) training complexity characteristics suitable for real-time application requirements. Deep learning approaches require $O(n^2)$ computational complexity but benefit substantially from Graphics Processing Unit acceleration capabilities. Ensemble methods scale linearly with base model quantity, requiring careful optimization between performance gains and computational resource overhead.

5. Challenges and Limitations

5.1. Dataset-Specific Limitations

The MLG-ULB dataset, despite being widely used, presents several important limitations [6]:

 doi:10.20944/preprints202507.1085.v1

- Principal Component Analysis (PCA) transformation removes raw feature values, limiting domain-specific feature engineering.
- The dataset covers only two days of transactions, preventing analysis of long-term fraud evolution.
- It includes only European cardholders, reducing generalizability to global scenarios.
- Fraud represents only 0.172% of all transactions, which may not reflect real-world class imbalance in other contexts.

5.2. Methodological Challenges

Key challenges identified in the reviewed studies include:

- Delays in fraud verification make real-time deployment difficult [7].
- Many models do not handle concept drift, making them less effective over time.
- Some studies focus heavily on accuracy, neglecting metrics like precision and recall [8].
- Cross-validation strategies vary widely, affecting result comparability.

5.3. Implementation Challenges

Real-world deployment of fraud detection models faces several technical and operational barriers:

- Real-time systems require response times under 100 milliseconds [27].
- Many models are not scalable to millions of transactions per day.
- Model interpretability is essential for audit and compliance in the financial sector.
- Reducing false positives is critical to avoid unnecessary customer disruptions and financial loss.

6. Future Research Directions

6.1. Immediate Opportunities

One of the most urgent research directions is the integration of explainable artificial intelligence (XAI) into fraud detection systems. Regulatory frameworks in the financial industry require transparency in model decisions, especially for customer-facing applications. Promising solutions include the use of SHAP and LIME with ensemble classifiers, visualization techniques for attention mechanisms in neural networks, and methods for rule extraction from black-box models. Developing interpretable models that do not compromise performance remains a key challenge.

Another important area is real-time optimization. As fraud detection systems must often operate within strict latency constraints, especially in high-frequency transaction environments, sub-millisecond inference is critical. Future work should focus on edge computing deployment strategies, continuous learning through streaming algorithms, and efficient hardware acceleration. Techniques such as model compression will also play a vital role in maintaining speed without sacrificing accuracy [27].

6.2. Advanced Methodological Directions

Federated learning offers a promising path for privacy-preserving collaboration between financial institutions [28]. Research in this area should focus on ensuring differential privacy, developing secure aggregation protocols, and handling heterogeneous data distributions across institutions. Improving communication efficiency will be crucial for enabling large-scale deployment of federated learning systems.

Another direction is multi-modal learning, which involves combining data from different sources to improve fraud detection accuracy. This includes fusing transaction records with behavioral biometrics, enabling transfer learning across different fraud domains, and integrating spatial-temporal information. Additionally, applying social network analysis can help identify coordinated fraud rings that may go undetected by single-channel methods.

 doi:10.20944/preprints202507.1085.v1

6.3. Emerging Technology Integration

Quantum computing is an emerging field that holds potential for solving complex fraud detection tasks. Future work should compare classical and quantum algorithms, explore hybrid quantum-classical models, and develop implementations suitable for near-term intermediate-scale quantum (NISQ) devices. Identifying areas where quantum advantage is achievable in fraud detection will be an important milestone.

Advancements in neural network design also offer opportunities. Graph Transformer Networks can model relational structures with attention mechanisms, while Neural Ordinary Differential Equations (ODEs) enable continuous-time modeling of transaction patterns. Meta-learning approaches could allow models to adapt quickly to new fraud types with limited data, and neuromorphic computing may enable ultra-efficient fraud detection on edge devices.

7. Conclusions

This review analyzed 52 studies on machine learning approaches for credit card fraud detection and identified clear performance trends across algorithm categories. Random Forest models with genetic algorithm-based feature selection achieved the highest reported accuracy, while ensemble methods showed strong robustness for real-world deployment. Deep learning models, particularly LSTM networks, were effective for capturing temporal patterns but required significant computational resources.

The analysis highlights four key findings: traditional machine learning methods are nearing performance limits; SMOTE preprocessing consistently improves results; ensemble techniques provide the best trade-off between accuracy and deployment feasibility; and emerging methods, such as quantum and graph-based models, are not yet practical for large-scale use.

Moving forward, research should shift from optimizing accuracy to solving deployment challenges. Priorities include integrating explainable AI, enabling real-time processing, and adopting privacy-preserving approaches like federated learning. Combining multiple techniques into hybrid models may offer the most effective solutions for next-generation fraud detection systems.

Appendix A. Additional Relevant References

The following references were reviewed during the study but were not directly cited in the main body of the paper. They are provided here to support further exploration by readers interested in credit card fraud detection using machine learning techniques.

[A1] 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, 2014.

[A2] C. Whitrow, D. J. Hand, P. Juszczak, D. Weston, and N. M. Adams, "Transaction aggregation as a strategy for credit card fraud detection," *Data Mining and Knowledge Discovery*, vol. 18, no. 1, pp. 30–55, 2016.

[A3] J. Jurgovsky, M. Granitzer, K. Ziegler, S. Calabretto, P.-E. Portier, L. He-Guelton, and O. Caelen, "Sequence classification for credit-card fraud detection," *Expert Systems with Applications*, vol. 100, pp. 234–245, 2017.

[A4] Y. Lucas, P.-E. Portier, L. Laporte, L. He-Guelton, O. Caelen, M. Granitzer, and S. Calabretto, "Credit card fraud detection using machine learning: A survey," arXiv preprint arXiv:1611.06439, 2017.

[A5] S. Misra, S. Thakur, M. Ghosh, and S. K. Saha, "Credit card fraud detection using computational intelligence techniques," in *2018 Int. Conf. on Information Technology (ICIT)*, pp. 1–6, IEEE, 2018.

[A6] B. Lebichot, T. Verhelst, Y.-A. Le Borgne, L. He-Guelton, F. Oblé, and G. Bontempi, "Transfer learning strategies for credit card fraud detection," *IEEE Access*, vol. 9, pp. 114754–114766, 2018.

[A7] V. R. Dornadula and S. Geetha, "Credit card fraud detection using machine learning algorithms," *Procedia Computer Science*, vol. 165, pp. 631–641, 2019.

[A8] A. Thennakoon, C. Bhagyani, S. Premadasa, S. Mihiranga, and N. Kuruwitaarachchi, "Real-time credit card fraud detection using machine learning," in *2019 9th Int. Conf. on Cloud Computing, Data Science & Engineering (Confluence)*, pp. 488–493, IEEE, 2019.

[A9] A. Pumsirirat and L. Yan, "Credit card fraud detection using deep learning based on auto-encoder and restricted Boltzmann machine," *Int. J. of Advanced Computer Science and Applications*, vol. 9, no. 1, pp. 18–25, 2019.

[A10] S. Khatri, A. Arora, and A. P. Agrawal, "Credit card fraud detection using machine learning models and collating machine learning models," *Int. J. of Pure and Applied Mathematics*, vol. 118, no. 20, pp. 825–838, 2020.

 doi:10.20944/preprints202507.1085.v1

[A11] N. Rtayli and N. Enneya, "Enhanced credit card fraud detection based on SVM-recursive feature elimination and hyper-parameters optimization," *J. of King Saud University - Computer and Information Sciences*, vol. 32, no. 9, pp. 1062–1070, 2020.
[A12] M. M. Hassan, A. Amanat, T. Ahmed, and M. M. Toma, "Credit card fraud detection using deep learning," *Int. J. of Computer Applications*, vol. 975, no. 8887, pp. 34–38, 2020.
[A13] K. Huang, "An optimized LightGBM model for fraud detection," *J. of Physics: Conf. Series*, vol. 1651, no. 1, p. 012111, 2021.
[A14] E. Duman and M. H. Ozcelik, "A cost-sensitive random forest approach for credit card fraud detection," *Expert Systems with Applications*, vol. 165, p. 113912, 2021.
[A15] T. H. Pranto, K. M. Hasib, T. Rahman, A. B. Haque, A. N. Islam, and R. M. Rahman, "Blockchain and machine learning for fraud detection: A privacy-preserving and adaptive incentive based approach," *IEEE Access*, vol. 10, pp. 87115–87134, 2021.
[A16] Y. Y. Festa and I. A. Vorobyev, "A hybrid machine learning framework for e-commerce fraud detection," *Model Assisted Statistics and Applications*, vol. 17, no. 1, pp. 41–49, 2021.
[A17] H. Chi, Y. Lu, B. Liao, L. Xu, and Y. Liu, "An optimized quantitative argumentation debate model for fraud detection in e-commerce transactions," *IEEE Intelligent Systems*, vol. 36, no. 2, pp. 52–63, 2021.
[A18] J. Forough and S. Momtazi, "Ensemble of deep sequential models for credit card fraud detection," *Applied Soft Computing*, vol. 99, p. 106883, Feb. 2021.
[A19] K. N. Mishra, V. P. Mishra, S. Saket, and S. P. Mishra, "Performance evaluation of machine learning methods for credit card fraud detection using SMOTE and AdaBoost," in *2021 Int. Conf. on Advances in Computing and Communications (ICACC)*, pp. 1–8, IEEE, 2021.
[A20] M. H. Nasr, M. H. Farrag, and M. M. Nasr, "A proposed fraud detection model based on e-payments attributes: A case study in Egyptian e-payment gateway," *Int. J. of Advanced Computer Science and Applications*, vol. 13, no. 5, pp. 179–186, 2022.
[A21] S. Dalal, B. Seth, M. Radulescu, C. Secara, and C. Tolea, "Predicting fraud in financial payment services through optimized hyper-parameter-tuned XGBoost model," *Mathematics*, vol. 10, no. 24, p. 4679, 2022.
[A22] E. K. Ampomah, Z. Qin, and G. Nyame, "Evaluation of tree-based ensemble machine learning models in predicting stock price direction of movement," *Information*, vol. 11, no. 6, p. 332, 2022.
[A23] D. H. Lim and H. Ahn, "A study on fraud detection in the C2C used trade market using Doc2vec," *Journal of Intelligence and Information Systems*, vol. 28, no. 1, pp. 27–44, 2022.
[A24] N. Drydakis, "Artificial intelligence and reducing business risk in SMEs: COVID-19 dynamic capacity analysis during a pandemic," *Information Systems Frontiers*, vol. 24, pp. 1223–1247, 2022.
[A25] A. Singh and A. Jain, "Credit card fraud detection using isolation forest technique," in *2022 Int. Conf. on Sustainable Computing and Data Communication Systems (ICSCDS)*, pp. 711–715, IEEE, 2022.
[A26] A. Abdallah, M. A. Maarof, and A. Zainal, "Imbalanced credit card fraud detection data: A solution based on hybrid neural network and clustering-based undersampling technique," *Applied Soft Computing*, vol. 132, p. 109830, 2023.

References

1. The Nilson Report, "Payment Card Fraud Losses Reach $32.34 Billion," Issue 1164, April 2019.
2. Association of Certified Fraud Examiners, "Report to the Nations: 2022 Global Study on Occupational Fraud and Abuse," 2022.
3. M. Homaei, A. C. Lindo, Ó. Mogollón-Gutiérrez, and J. D. Alonso, "The role of artificial intelligence in DT's cybersecurity," in *Proc. 17th Reunión Española sobre Criptología y Seguridad de la Información (RECSI)*, 2022, p. 133.3.
4. M. Homaei, Ó. Mogollón-Gutiérrez, J. C. Sancho, M. Ávila, and A. Caro, "A review of digital twins and their application in cybersecurity based on artificial intelligence," *Artificial Intelligence Review*, vol. 57, no. 8, Jul. 2024.
5. A. Dal Pozzolo, O. Caelen, Y.-A. Le Borgne, S. Waterschoot, and G. Bontempi, "Learned lessons in credit card fraud detection from a practitioner perspective," *Expert Systems with Applications*, vol. 41, no. 10, pp. 4915–4928, 2014.
6. A. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, "Credit card fraud detection: a realistic modeling and a novel learning strategy," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 29, no. 8, pp. 3784–3797, 2018.
7. F. Carcillo, A. Dal Pozzolo, Y.-A. Le Borgne, O. Caelen, Y. Mazzer, and G. Bontempi, "Scarff: a scalable framework for streaming credit card fraud detection with spark," *Information Fusion*, vol. 41, pp. 182–194, 2018.
8. T. Saito and M. Rehmsmeier, "The precision-recall plot is more informative than the ROC plot when evaluating binary classifiers on imbalanced datasets," *PLoS One*, vol. 10, no. 3, p. e0118432, 2015.
9. E. Ileberi, Y. Sun, and Z. Wang, "A machine learning based credit card fraud detection using the GA algorithm for feature selection," *Journal of Big Data*, vol. 9, no. 1, pp. 1–24, 2022.

 doi:10.20944/preprints202507.1085.v1

10. D. Varmedja, M. Karanovic, S. Sladojevic, M. Arsenovic, and A. Anderla, "Credit card fraud detection-machine learning methods," in *18th International Symposium INFOTEH-JAHORINA (INFOTEH)*, pp. 1–5, IEEE, 2019.
11. 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.
12. Y. Sahin, S. Bulkan, and E. Duman, "A cost-sensitive decision tree approach for fraud detection," *Expert Systems with Applications*, vol. 40, no. 15, pp. 5916–5923, 2013.
13. J. O. Awoyemi, A. O. Adetunmbi, and S. A. Oluwadare, "Credit card fraud detection using machine learning techniques: A comparative analysis," in *2017 International Conference on Computing Networking and Informatics (ICCNI)*, pp. 1–9, IEEE, Oct. 2017.
14. J. Li, S. Chen, and M. Wang, "A Deep Learning Method of Credit Card Fraud Detection Based on Continuous-Coupled Neural Networks," *Mathematics*, vol. 13, no. 5, p. 819, 2025.
15. I. D. Mienye and Y. Sun, "A deep learning ensemble with data resampling for credit card fraud detection," *IEEE Access*, vol. 11, pp. 30628–30638, 2023.
16. X. Zhang, Y. Han, W. Xu, and Q. Wang, "HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture," *Information Sciences*, vol. 557, pp. 302–316, 2021.
17. S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997.
18. M. Ahmed, S. Rahman, and M. S. Hossain, "Enhancing Credit Card Fraud Detection: An Ensemble Machine Learning Approach," *Big Data and Cognitive Computing*, vol. 8, no. 1, p. 6, 2024.
19. T. Chen and C. Guestrin, "Xgboost: A scalable tree boosting system," in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 785–794, 2016.
20. F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation forest," in *2008 Eighth IEEE International Conference on Data Mining*, pp. 413–422, IEEE, 2008.
21. M. M. Breunig, H.-P. Kriegel, R. T. Ng, and J. Sander, "LOF: identifying density-based local outliers," *ACM SIGMOD Record*, vol. 29, no. 2, pp. 93–104, 2000.
22. L. Ding, L. Liu, Y. Wang, P. Shi, and J. Yu, "An AutoEncoder enhanced light gradient boosting machine method for credit card fraud detection," *PeerJ Computer Science*, vol. 10, p. e2323, Oct. 2024.
23. M. El Alami, N. Innan, M. Shafique, and M. Bennai, "Comparative Performance Analysis of Quantum Machine Learning Architectures for Credit Card Fraud Detection," arXiv preprint arXiv:2412.19441, 2024.
24. S. Xiang, M. Zhu, D. Cheng, E. Li, R. Zhao, Y. Ouyang, L. Chen, and Y. Zheng, "Semi-supervised Credit Card Fraud Detection via Attribute-Driven Graph Representation," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 37, no. 12, pp. 14557–14565, June 2023.
25. C. Yu, Y. Xu, J. Cao, Y. Zhang, Y. Jin, and M. Zhu, "Credit Card Fraud Detection Using Advanced Transformer Model," in *2024 IEEE International Conference on Metaverse Computing, Networking, and Applications (MetaCom)*, pp. 343–350, IEEE, Aug. 2024.
26. N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, "SMOTE: synthetic minority over-sampling technique," *Journal of Artificial Intelligence Research*, vol. 16, pp. 321–357, 2002.
27. V. Soni, "Fraud Detection in Credit Card Transactions: A Machine Learning Approach," *Journal of Electrical Systems*, vol. 20, no. 11s, pp. 3938–3954, Nov. 2024.
28. M. Abdul Salam, K. M. Fouad, D. L. Elbably, and S. M. Elsayed, "Federated learning model for credit card fraud detection with data balancing techniques," *Neural Computing and Applications*, vol. 36, no. 11, pp. 6231–6256, Jan. 2024.