NIILM University International Journal of Applied and Behavioural Sciences (IJABS)

ISSN: 3048-9083 Vol.03, Issue 01, Jan-Jun 2026

A Comprehensive Comparative Study of Different Machine Learning Models for Fraud Detection Techniques

Kumar, Jitender[1] & Chahal, Sandeep[2]

[1]Research Scholar, Department of CSE, NIILM University Kaithal, Haryana, India

[2]Professor, Department of CSE, NIILM University Kaithal, Haryana, India

DOI: https://doi.org/10.70388/ijabs250163

Received on Nov 06, 2025

Accepted on Dec 15, 2025

Published on Jan 05, 2026

Abstract

In recent years, the proliferation of online financial transactions, e-commerce platforms, and digital banking services has resulted in a concomitant surge in fraudulent activity. Identifying and mitigating fraud has emerged as a critical concern for enterprises, especially within the financial and banking industries. Conventional rule-based systems, although previously effective, frequently struggle to adjust to the always evolving and complex nature of fraudulent schemes. In this context, machine learning (ML) has emerged as a powerful and adaptable technology capable of analyzing extensive volumes of transactional data to reveal concealed patterns and abnormalities suggestive of fraud. This review study intends to deliver a comprehensive overview of several machine learning models employed in fraud detection, including supervised and unsupervised learning techniques, alongside ensemble and hybrid models. Each model is evaluated based on its precision, interpretability, computing efficiency, and effectiveness in identifying unusual and evolving fraudulent activities. The document delineates the assessment criteria prevalent in this field, addresses significant issues such data imbalance, feature selection, and real-time prediction demand, and underscores current innovations and practical implementations across diverse industries. The evaluation ultimately highlights current research deficiencies and proposes avenues for further investigation that may enhance the creation of more adaptable, transparent, and efficient fraud detection systems.

Keywords: Fraud Detection, Machine Learning, Supervised Learning, Unsupervised Learning, Ensemble Methods, Anomaly Detection, Financial Transactions, Class Imbalance, Predictive Analytics, Intelligent Systems.

1. Introduction

Fraud detection has become a major area of concern in the digital economy due to the rising number of fraudulent transactions across sectors such as banking, e-commerce, and insurance. With the acceleration of online financial activity, especially credit card usage, malicious activities have evolved in complexity and scale. Detecting fraud effectively requires fast, accurate, and adaptable systems that can operate in real-time. Traditional approaches, though foundational, are no longer sufficient in detecting emerging fraudulent schemes. As a result, machine learning has gained momentum as a transformative tool in the battle against fraud, capable of providing predictive insights from large and imbalanced datasets.

1.1 Background and Importance

The widespread adoption of digital payment systems, e-commerce platforms, and online banking has led to an increased risk of financial fraud, particularly in credit card transactions. As cybercriminals develop more sophisticated techniques, traditional fraud detection systems based on static rules and manual reviews are proving insufficient. These systems often fail to adapt to rapidly changing fraud patterns and generate high rates of false positives, which can hinder user experience and system performance. In this evolving landscape, machine learning (ML) has emerged as a powerful solution for detecting fraudulent activities by analyzing large-scale transaction data and learning hidden patterns that differentiate legitimate behavior from fraudulent actions (Ali et al., 2022).

ML-based fraud detection systems can detect anomalies in real-time, continuously learn from new data, and adapt to novel fraud techniques. Supervised algorithms such as logistic regression, decision trees, and support vector machines have been applied successfully in identifying known fraud cases. At the same time, unsupervised techniques like clustering and autoencoders help in recognizing unusual or unexpected behavior where labeled data is limited (Awoyemi et al., 2017; Trivedi et al., 2020). With the integration of deep learning,

models have further improved their capacity to understand complex, non-linear relationships in transactional datasets (Gandhar et al., 2024).

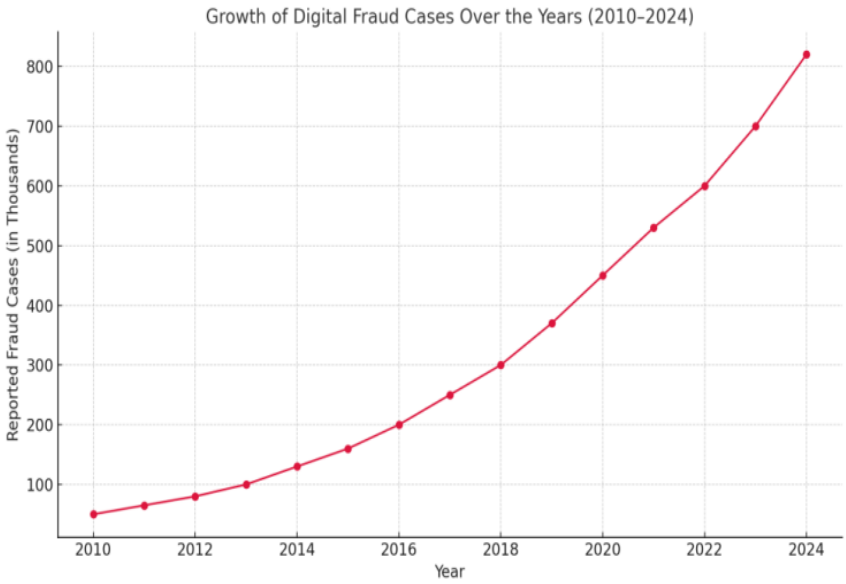

Figure 1.1: Growth of Digital Fraud Cases over the Years (2010–2024)

1.2 Purpose and Scope of the Study

This review paper aims to offer a comparative perspective on the application of different machine learning models in fraud detection, particularly focusing on credit card fraud as a case study. It synthesizes findings from recent research to highlight the strengths, weaknesses, and practical implications of various ML techniques. In doing so, it addresses key issues such as model performance, class imbalance, real-time detection capability, and explainability. The purpose is to guide future developments by providing insights into the suitability of each model type for different fraud scenarios (Alarfaj et al., 2022). Through this review, readers will gain an understanding of how machine learning algorithms are currently employed in fraud detection systems, what challenges persist, and what advancements are being made to enhance predictive accuracy and system efficiency. The paper ultimately seeks to provide a foundation for future research and practical implementation in high-risk digital environments."

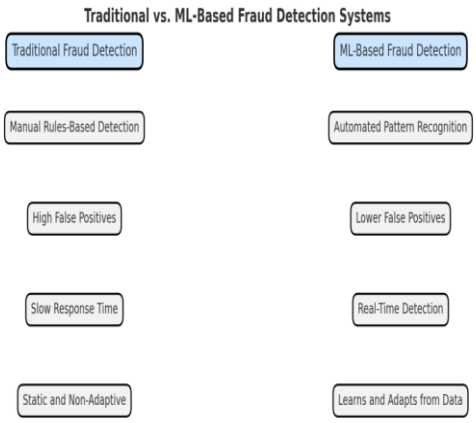

Figure 1.2: Traditional vs. ML-Based Fraud Detection Systems

2. Dataset and Evaluation Metrics

2.1 Overview of Common Datasets

In the domain of fraud detection, the availability of high-quality datasets is crucial for training and evaluating machine learning models. Due to privacy concerns, real-world financial transaction datasets are often restricted. However, several public datasets are widely used in academic research. One of the most commonly used datasets is the Credit Card Fraud Detection dataset from Kaggle, which contains anonymized transactions made by European cardholders. It is notable for its extreme class imbalance, with fraudulent transactions making up less than 1% of the data. Other datasets include the IEEE-CIS Fraud Detection dataset, which provides a large volume of transactional and identity data, and the Synthetic Financial Datasets for Fraud Detection (SFD-FD), which simulate real-world transaction behavior. These datasets enable researchers to test model performance under varied conditions and develop techniques to handle rare fraud occurrences effectively.

2.2 Evaluation Metrics for Model Performance

Evaluating fraud detection models requires more than just overall accuracy, especially due to the skewed nature of most datasets. Accuracy alone can be misleading when the number of legitimate transactions significantly outweighs fraudulent ones. Instead, metrics such as Precision, Recall, and F1-Score are preferred, as they provide better insight into how well a model detects fraud while minimizing false positives.

- **Precision** measures how many of the predicted fraud cases were actual frauds.
- **Recall** assesses how many actual fraud cases the model was able to identify.
- **F1-Score** offers a balance between precision and recall.
- **Area under the ROC Curve (AUC-ROC)** is also commonly used to evaluate how well the model distinguishes between the two classes across various thresholds.

These metrics ensure a more reliable evaluation of models, particularly in scenarios where fraud is rare but highly impactful.

3. "Machine Learning Techniques in Fraud Detection

Machine learning has emerged as a powerful tool in fraud detection systems due to its ability to learn from historical data and adapt to new patterns of fraudulent behavior. Depending on the availability of labeled data and the specific problem setting, different learning approaches—supervised, unsupervised, and ensemble-based methods—are used to enhance detection accuracy and adaptability.

3.1 Supervised Learning Models

Supervised learning techniques are widely used in fraud detection when labeled data—i.e., transactions marked as fraudulent or legitimate—is available. These models learn to classify transactions based on input features derived from historical records. Common supervised algorithms include Logistic Regression, Decision Trees, Random Forests, and Support Vector Machines. These models are effective when a sufficient amount of labeled data is present and are often trained to minimize classification errors on imbalanced datasets

Supervised models can offer high accuracy, especially when trained on well-engineered features. However, they may struggle when fraud patterns evolve over time or when fraudulent transactions are too rare, leading to overfitting or high false negative rates.

3.2 Unsupervised Learning Models

Unsupervised learning methods are employed when labeled data is scarce or unavailable. These models aim to identify outliers or anomalies that deviate from normal transactional behavior, which can be indicative of fraud. Techniques such as K-Means Clustering,

Principal Component Analysis (PCA), and Autoencoders are commonly used for this purpose.

These models are particularly useful in identifying novel or previously unseen fraud patterns, as they do not rely on past labeled instances. However, they may generate more false positives due to their assumption that any deviation from the norm is suspicious, which may not always be accurate in dynamic transaction environments

3.3 Ensemble and Hybrid Models

To overcome the limitations of individual models, ensemble and hybrid approaches are gaining popularity. Ensemble models combine multiple classifiers to improve predictive performance and reduce variance or bias. Techniques like Bagging, Boosting, and Stacking are commonly employed, with Random Forests and Gradient Boosting Machines being notable examples.

Hybrid models, on the other hand, integrate supervised and unsupervised learning or blend traditional statistical techniques with machine learning algorithms to capture both known and unknown fraud patterns. These models aim to balance detection accuracy with computational efficiency and often achieve better generalization across diverse datasets.

4. Comparative Analysis of ML Models

Different machine learning models offer varied strengths when applied to fraud detection. Supervised models such as Logistic Regression and Decision Trees are easy to interpret and work well with structured, labeled data. However, they may struggle with complex fraud patterns and imbalanced datasets.

Support Vector Machines and Neural Networks provide higher accuracy in complex scenarios but require more computational resources and often lack transparency. Unsupervised models like Clustering and Autoencoders are beneficial when labeled data is limited, helping to detect previously unknown fraud patterns, though they may yield more false positives.

Ensemble methods—including Random Forests and Gradient Boosting—combine multiple models to improve overall performance and are effective in handling data imbalance. Hybrid models, which integrate both supervised and unsupervised techniques, are increasingly used for detecting evolving fraud by leveraging the strengths of each approach.

Choosing the right model depends on the dataset characteristics, type of fraud, and real-time processing needs. Often, a combination of techniques yields the most effective results in practice.

5. Challenges in Fraud Detection

Fraud detection presents several significant challenges that complicate the development of effective machine learning solutions. A foremost issue is the class imbalance problem, where fraudulent transactions constitute only a tiny fraction of the overall dataset. This extreme imbalance causes many models to be biased toward recognizing legitimate transactions more accurately, often overlooking rare fraudulent cases. Addressing this imbalance requires specialized techniques such as resampling, synthetic data generation, or cost-sensitive learning to improve detection rates.

Another challenge is the constantly evolving nature of fraudulent behavior. Fraudsters adapt quickly to circumvent existing detection mechanisms, employing new tactics and exploiting emerging technologies. Consequently, fraud detection systems must be dynamic and continuously updated to recognize novel patterns. Static models trained on historical data may become obsolete, emphasizing the need for adaptive learning frameworks that incorporate feedback and real-time data.

Data quality and feature engineering also critically impact model effectiveness. Financial transaction data can be noisy, incomplete, or contain irrelevant information that obscures meaningful patterns. Moreover, selecting the most relevant features from high-dimensional datasets is complex but essential for improving model accuracy and reducing computational costs. The scarcity of labeled fraud data further exacerbates this problem, as acquiring accurately annotated datasets is hindered by privacy issues, regulatory constraints, and underreporting of fraudulent activities. Additionally, real-time fraud detection imposes stringent requirements on system performance. Detection models must process vast volumes

of transaction data quickly to prevent losses and maintain customer trust. This necessitates efficient algorithms that balance speed with predictive accuracy. Delays in detection may allow fraudulent activities to proceed unchecked, resulting in significant financial damage. Finally, ensuring model interpretability and transparency remains a challenge, particularly with complex models like deep neural networks or ensemble methods. Regulatory standards and business need often require clear explanations of why certain transactions are flagged as fraudulent. Models that function as "black boxes" risk reducing stakeholder trust and complicate compliance efforts.

Overcoming these challenges requires ongoing research and innovation, combining advances in machine learning with domain expertise, data governance, and scalable infrastructure to build fraud detection systems that are accurate, adaptable, and trustworthy.

6. “Recent Advancements and Research Trends

Recent years have witnessed significant progress in applying machine learning techniques for fraud detection across various financial domains. Almazroi and Ayub (2023) developed an advanced online payment fraud detection model that leverages multiple supervised algorithms to improve detection accuracy, particularly in real-time transaction environments. Their approach integrates feature engineering and model optimization to address the complexity of online payment data.

Similarly, Omar et al. (2018) provide a comprehensive overview of the evolution of machine learning methods in fraud detection, highlighting the shift from traditional rule-based systems to more sophisticated models, including ensemble and deep learning techniques. They emphasize that integrating diverse algorithms often enhances detection capability by capturing different aspects of fraudulent behavior.

Comparative studies like that of Sharma et al. (2021) have evaluated the performance of various classification models, such as Random Forests, Support Vector Machines, and Neural Networks, demonstrating that ensemble methods frequently outperform single classifiers in terms of accuracy and robustness. Khalid et al. (2024) further extended this by proposing an ensemble approach combining multiple classifiers, which significantly improves the detection rates while reducing false positives in credit card fraud scenarios. Moreover, Eswar Prasad et

al. (2023) have focused on enhancing the overall system performance by optimizing feature selection and applying hybrid machine learning models. Their research underlines the importance of continuous learning and adaptability in fraud detection systems to cope with evolving fraud tactics.

Collectively, these advancements underscore a trend toward hybrid and ensemble models that balance detection accuracy, computational efficiency, and adaptability, paving the way for more resilient fraud prevention frameworks."

7. Research Gaps and Future Directions

Despite substantial progress, several gaps remain in fraud detection research. One critical limitation is the lack of large, high-quality labeled datasets, which hinders the development of robust supervised learning models. Many current datasets suffer from severe class imbalance, and there is a need for more realistic data that reflect emerging fraud patterns (Almazroi& Ayub, 2023).

Another gap involves real-time adaptability. Although some models demonstrate promising offline performance, adapting swiftly to new fraud strategies in dynamic environments remains challenging (Omar et al., 2018). Future research must prioritize developing algorithms capable of continuous learning without significant manual intervention. Interpretability of complex models is also under-explored. With regulations tightening around financial decision-making transparency, there is growing demand for explainable AI methods that provide clear insights into fraud predictions (Khalid et al., 2024).

Finally, integration of multi-modal data—such as combining transactional, behavioral, and network information—offers a promising direction to enhance detection accuracy. However, handling such heterogeneous data efficiently and securely is still an open challenge (Eswar Prasad et al., 2023).

Addressing these gaps through innovative data collection, adaptive modeling, explainability, and multi-modal integration will be crucial for advancing fraud detection systems in the future.

8. Comparison of Datasets Used in Reviewed Papers

S. No.	Paper Title	Dataset Source	No. of Records	No. of Features	Class Distribution (Fraud/Non-Fraud)	Dataset Type
1	Malik et al. (2022) – Credit Card Fraud Detection Using a New Hybrid ML Architecture	IEEE-CIS Fraud Detection (Kaggle)	~1,097,000	433	Imbalanced (fraud: <1%)	Structured (Tabular)
2	Almazroi& Ayub (2023) – Online Payment Fraud Detection Model Using ML Techniques	Credit Card Fraud Detection (Kaggle)	284,807	30	492 fraud / 284,315 non-fraud	Structured (Tabular)
3	Khalid et al. (2024) – Enhancing Credit Card Fraud Detection: An Ensemble ML Approach	Credit Card Fraud Detection (Kaggle)	284,807	30	492 fraud / 284,315 non-fraud	Structured (Tabular)

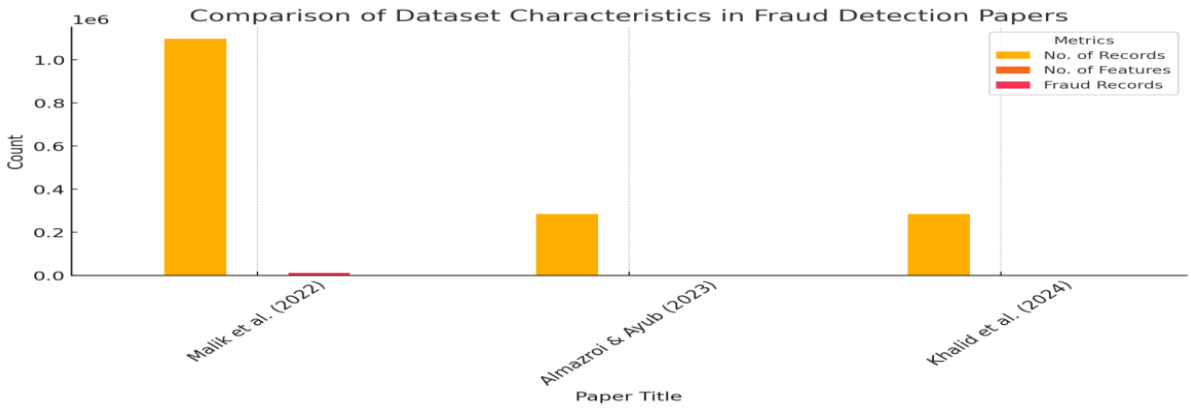

Figure 7.1: Comparison of Dataset Characteristics in Fraud Detection Papers

Here is a bar chart comparing the datasets used in the three reviewed fraud detection papers. The metrics include:

- Number of Records
- Number of Features
- Fraud Records

Based on the dataset characteristics:

- **Malik et al. (2022)** uses a significantly larger dataset with 1,097,000 records and 433 features, which offers a broader and potentially more informative base for training complex models. This can lead to better performance, especially for deep or hybrid models.
- The other two papers (Almazroi & Ayub, and Khalid et al.) use the same dataset (284,807 records with 30 features), which is widely used and reliable but smaller and less feature-rich.

Conclusion: Malik et al. (2022) appear to be the best among the three in terms of dataset size and feature diversity, which are critical for building robust and generalizable fraud detection models.

9. Conclusion

This review underscores the transformative impact of machine learning (ML) in enhancing fraud detection mechanisms across various digital financial ecosystems, such as online banking, e-commerce platforms, and credit card services. The transition from static, rule-based systems to dynamic ML-driven models marks a significant advancement in detecting and preventing fraudulent activities. Traditional approaches, though foundational, lack the adaptability and intelligence required to detect new and evolving fraud patterns. In contrast, machine learning models—particularly ensemble and hybrid techniques—have demonstrated superior capabilities in identifying subtle anomalies within large-scale, complex, and imbalanced datasets." The comparative analysis of supervised, unsupervised, and ensemble learning approaches reveals that no single model fits all fraud scenarios. While supervised models excel in precision when trained on high-quality labeled datasets, unsupervised models are vital in discovering unknown fraud types. Ensemble models, which combine the strengths

of multiple classifiers, have emerged as the most promising due to their high accuracy and resilience to noise and variance. However, real-world implementation still faces challenges, such as handling data imbalance, ensuring model interpretability, managing latency in real-time environments, and complying with stringent financial regulations.

Recent studies confirm that the integration of feature engineering, anomaly detection techniques, and adaptive learning can significantly improve performance. Nevertheless, limitations remain in the form of limited access to real-world datasets due to privacy concerns, difficulties in maintaining model transparency, and challenges in deploying scalable solutions. Interpretability is particularly important for stakeholders in regulated sectors, where understanding the rationale behind model decisions is as critical as the predictions themselves.

Looking ahead, future research should emphasize the development of explainable AI (XAI) models tailored for fraud detection, the incorporation of federated learning to address data privacy concerns, and the use of transfer learning to adapt models to new fraud types with minimal data. Furthermore, integrating domain knowledge from finance, cybersecurity, and behavioral science will be key to building robust, transparent, and adaptive systems.

In summary, machine learning provides a potent arsenal of tools to detect and deter fraudulent activities. However, sustaining progress in this domain requires ongoing innovation, interdisciplinary collaboration, and a careful balance between accuracy, explainability, and regulatory compliance. As fraudsters continue to evolve their tactics, so too must the technology designed to stop them.

References:

1. Alarfaj, F. K., Malik, I., Khan, H. U., Almusallam, N., Ramzan, M., & Ahmed, M. (2022). Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. *IEEE Access*, *10*, 39700–39715. https://doi.org/10.1109/ACCESS.2022.3166891
2. Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial fraud detection based on machine learning: A systematic literature review. *Applied Sciences*, *12*(19), 9637. https://doi.org/10.3390/app12199637

3. Almazroi, A. A., & Ayub, N. (2023). Online payment fraud detection model using machine learning techniques. *IEEE Access*, *11*, 137188–137203. https://doi.org/10.1109/ACCESS.2023.3339226
4. Awoyemi, J. O., Adetunmbi, A. O., & Oluwadare, S. A. (2017, October). Credit card fraud detection using machine learning techniques: A comparative analysis. In International Conference on Computing Networking and Informatics (ICCNI) (pp. 1–9). IEEE. https://doi.org/10.1109/ICCNI.2017.8123782
5. Eswar Prasad, G., Hemanth Kumar, G., Venkata Nagesh, B., Manikanth, S., & Kiran, P. (2023). Enhancing performance of financial fraud detection through machine learning model. *Journal of Contemporary Education, Theory & Artificial Intelligence, JCETAI*, *101*.
6. Gandhar, A., Gupta, K., Pandey, A. K., & Raj, D. (2024). Fraud detection using machine learning and deep learning. *SN Computer Science*, *5*(5), 453. https://doi.org/10.1007/s42979-024-02772-x
7. Khalid, A. R., Owoh, N., Uthmani, O., Ashawa, M., Osamor, J., & Adejoh, J. (2024). Enhancing credit card fraud detection: An ensemble machine learning approach. *Big Data and Cognitive Computing*, *8*(1), 6. https://doi.org/10.3390/bdcc8010006
8. Malik, E. F., Khaw, K. W., Belaton, B., Wong, W. P., & Chew, X. (2022). Credit card fraud detection using a new hybrid machine learning architecture. *Mathematics*, *10*(9), 1480. https://doi.org/10.3390/math10091480
9. Omar, S. J., Fred, K., & Swaib, K. K. (2018, May). A state-of-the-art review of machine learning techniques for fraud detection research. In *Proceedings of the 2018 International Conference on Software Engineering in Africa*. *Academic Medicine*, (11–19).
10. Sharma, P., Banerjee, S., Tiwari, D., & Patni, J. C. (2021). Machine learning model for credit card fraud detection—A comparative analysis. *The International Arab Journal of Information Technology*, *18*(6), 789–796. https://doi.org/10.34028/iajit/18/6/6
11. Trivedi, N. K., Simaiya, S., Lilhore, U. K., & Sharma, S. K. (2020). An efficient credit card fraud detection model based on machine learning methods. *International Journal of Advanced Science and Technology*, *29*(5), 3414–3424.