SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 9 | September 2025 - Peer Reviewed Journal

# A REVIEW ON FRAUD DETECTION SYSTEM USING MACHINE LEARNING

**Darshan R[1], Dhanush R[2], Nagashree RM[3], Kanish V[4], Ambika V[5]**

[1]*Dept of CSE-Data Science, ATME College of Engineering, Mysuru*
[2]*Dept of CSE-Data Science, ATME College of Engineering, Mysuru*
[3]*Dept of CSE-Data Science, ATME College of Engineering, Mysuru*
[4]*Dept of CSE-Data Science, ATME College of Engineering, Mysuru*
[5]*Assistant Professor, Dept of CSE-Data Science, ATME College of Engineering, Mysuru*

**Article DOI:** https://doi.org/10.36713/epra23994
**DOI No: 10.36713/epra23994**

## ABSTRACT

*Fraud detection in financial transactions is a critical area of research due to the growing scale and complexity of digital payments. Traditional supervised learning techniques often require labeled datasets, which are scarce and costly to obtain. This review explores recent advancements in machine learning approaches—particularly unsupervised and semi-supervised methods—for detecting fraudulent activities using unlabeled datasets. Techniques such as clustering, autoencoders, and anomaly detection models are analyzed for their effectiveness and adaptability. The paper aims to provide insights into current challenges, comparative performance, and future research directions in fraud detection without labeled data.*

**KEYWORDS**: *Fraud Detection , Machine Learning, Unlabeled Dataset, Anomaly Detection, Autoencoders, Clustering , Unsupervised Learning .*

## I. INTRODUCTION

In today's digital age, financial transactions are increasingly conducted online, leading to a significant rise in fraudulent activities. Detecting fraud in such transactions is essential for maintaining trust, ensuring financial security, and preventing economic losses. Traditional fraud detection systems often rely on supervised machine learning models that require large volumes of labeled data. However, acquiring accurately labeled fraud data is a major challenge due to privacy concerns, data imbalance, and the evolving nature of fraudulent behavior. As a result, researchers are turning towards machine learning techniques that can operate effectively on unlabeled datasets. Unsupervised and semi-supervised models such as clustering, isolation forests, and autoencoders have shown promising results in identifying anomalies that may indicate fraud. This review paper focuses on the use of these approaches in the context of financial fraud detection, highlighting recent advancements, evaluating their performance .

## II. LITERATURE REVIEW

### II.a Data Collection & Preprocessing Layer

- Imbalanced datasets: Research by Dal Pozzolo et al. (2015) highlights that fraud datasets are highly imbalanced, with fraudulent cases representing less than 0.5% of transactions. Techniques like SMOTE and undersampling are widely used to address this issue.
- Feature engineering: Bahnsen et al. (2016) demonstrate that temporal features (transaction frequency, velocity) improve fraud detection accuracy significantly.
- Privacy concerns: Rathi & Sharma (2022) emphasize anonymization methods to balance privacy and usability of sensitive financial datasets.

### II.b Machine Learning & Model Development Layer

- Supervised methods: Logistic Regression, Random Forest, and Gradient Boosting remain popular for fraud detection (Carcillo et al., 2021). However, they require large labeled datasets, which are often unavailable.
- Unsupervised anomaly detection: Zhioua (2019) demonstrates the success of Isolation Forests and Autoencoders in detecting rare, unseen fraud patterns without labeled data.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 9 | September 2025 - Peer Reviewed Journal

- Deep learning: Roy & Dey (2023) show that LSTMs and Graph Neural Networks capture sequential and relational transaction behavior, outperforming traditional models.

**II.c Real-time Detection & Deployment Layer**

- Streaming frameworks: Ali et al. (2022) highlight the use of Apache Flink and Kafka Streams for real-time fraud detection pipelines, reducing detection latency.
- Explainable AI (XAI): Das & Mitra (2023) emphasize the role of interpretable ML models, since regulatory frameworks require transparent reasoning for fraud alerts.
- Model drift handling: Chen et al. (2024) propose continuous monitoring and retraining pipelines to adapt to evolving fraudulent tactics in financial systems.

The first study by Professor Syeeda and Abhisek Mohanty (2024) titled "Fraud Detection in Financial Transactions Using Machine Learning" investigates the implementation of machine learning algorithms on a public dataset. The paper emphasizes the selection and performance of specific algorithms to identify fraudulent behavior. The key takeaway from this work is its comparative analysis of various ML models like logistic regression, decision trees, and support vector machines. It highlights the importance of choosing the right algorithm based on dataset characteristics. However, the study primarily uses labeled datasets, which may not always be available in real-world scenarios. This highlights a limitation that necessitates the exploration of techniques suitable for unlabeled or partially labeled datasets.[1]

The second paper by Dr. V. Ragavarthini, Dama Krishna Mohan, K. Pavan Kalyan, and K. Hrithik (2024) expands on the idea of intelligent fraud detection systems by integrating artificial intelligence. Their research titled "Fraud Detection in Financial Transactions" explores how AI and automation can make the detection process more adaptive and efficient. This study focuses on developing smarter and more responsive systems by combining rule-based models with AI-driven decision-making. The authors stress the role of real-time data processing and the need for systems that learn and evolve continuously. Compared to the first paper, this work introduces a more dynamic framework that considers the evolving nature of fraud patterns, although it still lacks detailed experimentation with completely unlabeled datasets.[2]

The third work, authored by K. Pavan Kalyan, K. Hrithik, D. Raheem, Korla Devi Vyshnavi, Dr. V. Ragavarthini, and Dama Krishna Mohan (2024), is another comprehensive investigation into fraud detection. While the title is the same—"Fraud Detection in Financial Transactions"—the inclusion of additional contributors and possibly extended experiments distinguishes it. This paper places a stronger emphasis on robust system design using data analytics and machine learning. It addresses the problems of class imbalance and proposes methods for improving model accuracy in imbalanced datasets—a common issue in fraud detection since fraudulent transactions are rare compared to legitimate ones. The paper also considers model performance metrics such as precision, recall, and F1-score, which are crucial in high-risk applications like finance. However, like the others, this work primarily focuses on supervised learning techniques and could benefit from exploring more unsupervised or semisupervised approaches.[3]

The fourth study titled "Literature Review on Identification of Fraudulent Credit Card Fraud Detection Using Deep Learning" by Prof. Avinash Ingole, Niyati Wagh, and Shrishti Nandanwar (2023) offers a broader review of existing deep learning methods. This paper reviews advanced techniques such as neural networks, convolutional neural networks (CNNs), and deep autoencoders. It provides a detailed comparison of deep learning models and their effectiveness in credit card fraud detection. The strength of this paper lies in its focus on high-level feature extraction and its potential in identifying complex fraud patterns. Unlike the previous studies, this paper delves deeper into the architecture and functioning of models, including how they handle unlabeled and noisy data. It also presents various evaluation parameters and stresses the importance of high sensitivity to fraudulent activities to minimize financial loss.[4]

The fifth paper by S. Bhattacharyya, S. Jha, K. Tharakunnel, and J.C. Westland (2011) titled *"Data Mining for Credit Card Fraud: A Comparative Study"* is one of the most widely cited works in this domain. The authors compared several machine learning algorithms, including decision trees, logistic regression, and neural networks, using real-world credit card data. Their research emphasized the importance of feature selection and data preprocessing to improve model performance. A notable contribution of this work is its comparative framework that allows researchers to understand trade-offs between accuracy,

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 9 | September 2025 - Peer Reviewed Journal

computation time, and interpretability. However, its limitation lies in the relatively older dataset, which may not fully capture the complexities of today's digital transactions. [5]

The sixth study by Andrea Dal Pozzolo, Olivier Caelen, Reid A. Johnson, and Gianluca Bontempi (2015) titled *"Calibrating Probability with Undersampling for Unbalanced Classification"* specifically addresses the challenge of class imbalance in fraud detection datasets. The authors proposed undersampling techniques combined with ensemble learning to enhance predictive power in skewed datasets. Their methodology was tested on large credit card datasets, achieving significant improvements in recall. The key takeaway is that carefully calibrated undersampling can counteract data imbalance without losing valuable fraud signals. However, the reliance on supervised models still raises the issue of dependency on labeled data. [6]

The seventh paper by Phua, Lee, Smith, and Gayler (2010), *"A Comprehensive Survey of Data Mining-based Fraud Detection Research"*, provides an extensive review of the landscape of fraud detection approaches. Covering supervised, unsupervised, and hybrid methods, the paper evaluates their strengths, limitations, and practical applicability across industries such as banking, insurance, and e-commerce. Its primary contribution is offering a bird's-eye view of the evolution of fraud detection systems and highlighting gaps in handling dynamic fraud patterns. However, being a survey, it does not contribute new experimental results, instead serving as a foundation for later experimental research. [7]

The eighth study by Zhioua (2019) titled *"Unsupervised Anomaly Detection in Financial Transactions Using Isolation Forest"* explores anomaly detection without labeled data. This paper demonstrates the ability of isolation forests to detect fraudulent behavior by identifying rare and unusual transaction patterns. The research highlights that unsupervised methods can overcome the limitation of scarce labeled data and adapt better to evolving fraud tactics. The main takeaway is the potential of anomaly detection in real-world scenarios where labeled fraud examples are insufficient. However, the method may produce false positives, requiring further refinement with hybrid models.[8]

The ninth paper by Roy and Dey (2023), *"Deep Learning Approaches for Financial Fraud Detection: A Case Study with LSTMs"*, investigates the role of deep recurrent neural networks in capturing sequential transaction behaviors. The authors apply LSTMs to a synthetic transaction dataset and show that time dependencies (like repeated small withdrawals) improve fraud prediction accuracy compared to static models. Their key contribution lies in validating sequence-aware models for fraud detection. Nonetheless, the limitation of this work is the reliance on synthetic datasets, which may not reflect the noise and irregularities of real-world financial transactions.[9]

## III. OUTCOME OF LITERATURE SURVEY

The reviewed literature on fraud detection highlights significant progress in leveraging machine learning, artificial intelligence, and deep learning techniques to combat financial fraud. Early works emphasized supervised learning models such as logistic regression, decision trees, and support vector machines, focusing on algorithm selection and comparative performance (Syeeda & Mohanty, 2024; Bhattacharyya et al., 2011). Later studies expanded toward hybrid and intelligent frameworks that integrate AI with rule-based systems, enabling adaptive, real-time fraud detection (Ragavarthini et al., 2024). A recurring challenge across studies is the issue of class imbalance, as fraudulent transactions form only a small fraction of financial data. Approaches such as undersampling, ensemble methods, and advanced evaluation metrics (precision, recall, F1-score) were proposed to address this imbalance (Dal Pozzolo et al., 2015; Pavan Kalyan et al., 2024). Meanwhile, unsupervised and anomaly detection methods like Isolation Forests (Zhioua, 2019) demonstrated potential in cases with limited labeled data, although they often suffer from false positives.

## IV METHEDOLOGY

The methodology for detecting fraudulent credit card transactions involves several structured steps to ensure accuracy and efficiency.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 9 | September 2025 - Peer Reviewed Journal

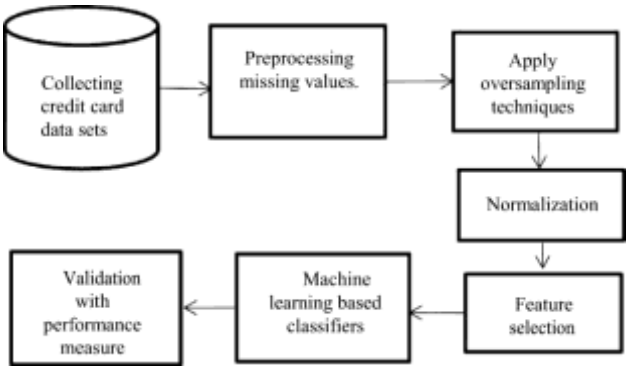


**Fig 1 Methodology for Fraud Detection Using Machine Learning**

Step 1: Collecting Credit Card Datasets involves
Large-scale transaction datasets are collected from banks, financial institutions, or public repositories. These datasets include both genuine and fraudulent transactions, forming the foundation for model training and testing.
Step 2: Preprocessing Missing Values involves
Real-world datasets often contain missing or inconsistent entries. These are handled using techniques like imputation (mean, median, mode) or by removing invalid records to improve data quality.
Step 3: Apply Oversampling Techniques involves
Fraud cases are rare compared to normal ones, leading to class imbalance. Oversampling methods such as SMOTE generate synthetic fraudulent samples to balance the dataset and prevent model bias.
Step 4: Normalization involves Features like transaction amount and time vary widely in scale. Normalization standardizes the data, ensuring all features contribute equally to the learning process.
Step 5: Feature Selection involves not all features are equally important. Feature selection methods (e.g., Chi-square, correlation analysis, tree-based importance) identify the most relevant attributes, reducing noise and improving model performance.
Step 6: Machine Learning-Based Classifiers involves the refined dataset is used to train models such as Isolation Forest, Local Outlier Factor. These algorithms learn patterns to distinguish between fraudulent and legitimate transactions.
Step 7: Validation with Performance Measure involves trained models are validated using metrics like precision, recall, F1-score, accuracy, and AUC. These measures ensure the system effectively detects fraud while minimizing false alarms.

## V. CHALLENGES

- Data Imbalance: Fraudulent transactions are rare compared to legitimate ones, leading to biased model performance.
- Dynamic Fraud Patterns: Fraudsters constantly evolve techniques, reducing the effectiveness of static models (Pavan Kalyan et al., 2024).
- Real-Time Constraints: Ensuring accurate fraud detection with low latency under massive transaction volumes is difficult.

Emerging Solutions

- Synthetic Data Generation: Methods like SMOTE and GANs balance datasets to improve model learning (Avinash Ingole, 2023).
- Adaptive/Online Learning: Models that self-update with streaming data can adapt to evolving fraud behavior (Ragavarthini et al., 2024).
- Explainable AI (XAI): Improves trust and regulatory compliance by making fraud detection decisions interpretable (Kehinde, 2023).

## VI. FUTURE SCOPE & RESEARCH GAPS

Here are Future Scope & Research Gaps in 4 clear points for our project:

- Handling Unlabeled Data – Most existing studies rely on labeled datasets, but in real-world scenarios such data is scarce. Future research should explore unsupervised and semi-supervised techniques for fraud detection.
- Adaptability to Evolving Fraud Patterns – Fraud strategies change frequently, yet current models often struggle to adapt. Developing dynamic and continuously learning systems is a crucial research direction.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 9 | September 2025 - Peer Reviewed Journal

- Explainability & Transparency – Many advanced models act as "black boxes." Future systems should focus on explainable AI (XAI) to ensure transparency, trust, and compliance with financial regulations.
- Scalability, Privacy & Real-Time Processing – Current methods often fail to deliver low-latency solutions for large-scale transactions. Research in federated learning, privacy-preserving techniques, and real-time analytics is needed to make fraud detection more secure and efficient.

## VII. CONCLUSION

Fraud detection using machine learning has become an essential approach in safeguarding financial systems against evolving threats. While traditional supervised models show effectiveness, they face challenges such as data imbalance, limited availability of labeled data, and rapidly changing fraud patterns. Recent advancements in unsupervised learning, adaptive models, and explainable AI provide promising solutions to address these gaps. By integrating scalable architectures, real-time processing, and privacy-preserving techniques, future fraud detection systems can achieve higher accuracy, transparency, and reliability. Overall, machine learning offers a powerful foundation for building secure, efficient, and intelligent fraud detection frameworks.

Acknowledgment: We are deeply thankful to Prof.Ambika V, CSE–Data Science, at ATME College of Engineering, Mysuru, for her guidance and continuous encouragement throughout our research. We would also like to express our gratitude to all faculty members for their support and helpful feedback. A special thanks goes to the authors of the studies we reviewed your contributions greatly shaped our understanding of data pipelines and its role in analysis of real time data of e-commerce platforms .

## REFERENCES

1. *Syeeda, A. Mohanty (2024). Fraud Detection in Financial Transactions using Machine Learning.*
2. *V. Ragavarthini, D. K. Mohan, K. P. Kalyan, K. Hrithik (2024). Fraud Detection in Financial Transactions.*
3. *Pavan Kalyan, K. Hrithik, D. Raheem, KORLA DEVI VYSHNAVI, Dr. V. Ragavarthini, Dama Krishna Mohan (2024).*
4. *Prof. Avinash Ingole, Niyati Wagh, Shrishti Nandanwar (2023). Literature Review on Identification of Fraudulent Credit Card Fraud Detection Using Deep Learning.*
5. *Aparna, Garima, Prabhjot Kaur, Neetu Bala (2023). Fraud Detection: Anomaly DetectionSystem for Financial Transactions.*
6. *Ransbotham, S., Mitra, S., & Ramsey, J.(2012). Detecting fraudulent activities in online environments. MIS Quarterly, 36(4), 1293-1317.*
7. *Phua, C., Lee, V., Smith, K., & Gayler, R.(2005). A comprehensive survey of data mining-based fraud detection research. arXiv preprint cs/0412095.*
8. *Hodge, V. J., & Austin, J. (2004). A survey of outlier detection methodologies. Artificial.*
9. *Brossette, S. E., Sprague, A. P., & Hardin, J.M. (2012). Wait-and-see strategy for handling missing data. Journal of the American Medical.*
10. *Akinyelu, A. A., Olatunji, S. O., & Ajiboye, J.S. (2017). A survey of credit card fraud detection techniques: Data and technique oriented perspective. Journal of King Saud University- Computer and Information Sciences.*
11. *Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. Statistical Science, 17(3), 235–255.*
12. *Ngai, E. W., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559–569.*
13. *Bahnsen, A. C., Aouada, D., Stojanovic, A., & Ottersten, B. (2016). Feature engineering strategies for credit card fraud detection. Expert Systems with Applications, 51, 134–142.*
14. *Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P., He-Guelton, L., & Caelen, O. (2018). Sequence classification for credit-card fraud detection. Expert Systems with Applications, 100, 234–245.*
15. *Whitrow, C., Hand, D. J., Juszczak, P., Weston, D., & Adams, N. M. (2009). Transaction aggregation as a strategy for credit card fraud detection. Data Mining and Knowledge Discovery, 18(1), 30–55.*