© November 2025 | IJIRT | Volume 12 Issue 6 | ISSN: 2349-6002

AI Based Transaction Anomaly and Fraud Detection System

Ms. Sana Mohammad Sadique Shaikh[1], Mr. Goden N.A.[2]
[1,2] V.V.P Institute of Engineering and Technology, Solapur, Maharashtra, India.

Abstract—**The rapid growth of digital payments has significantly increased the number of fraudulent online transactions. Traditional fraud detection systems rely on predefined rules, which makes them ineffective in identifying new, complex, and evolving fraud patterns. To address this challenge, this research proposes an AI-based Transaction Anomaly and Fraud Detection System that analyzes user behavior, spending patterns, temporal features, merchant categories, and location-based signals to detect suspicious activities. The system utilizes machine learning and anomaly detection techniques, including Isolation Forest and XGBoost, to classify transactions and assign a risk score. Additionally, explainable AI methods are integrated to provide the reason behind each flagged transaction, ensuring transparency and trust. A dashboard is designed for real-time monitoring, visualization, and decision-making. This work aims to build a scalable, accurate, and intelligent fraud detection framework suitable for banking and financial sectors. Implementation and evaluation of the proposed model will be carried out in subsequent phases.**

Index Terms—**Fraud Detection, Anomaly Detection, Machine Learning, XGBoost, Risk Scoring**

I. INTRODUCTION

In today's digitally driven financial landscape, the rise of online banking, e-commerce platforms, and electronic payment systems has significantly transformed the way monetary transactions are conducted. However, this rapid digital expansion has also made financial systems increasingly vulnerable to sophisticated fraud attempts. Fraudulent transactions now represent a major threat to individuals, businesses, and financial institutions, as cybercriminals employ advanced techniques to exploit system vulnerabilities and manipulate transaction channels for unauthorized financial gain. These fraudulent activities often involve identity theft, account compromise, unauthorized payment requests, and other deceptive methods designed to illegally divert funds or access confidential information[1–10].
To address these growing risks, financial organizations are progressively adopting Artificial Intelligence (AI) and Machine Learning (ML) technologies to enhance fraud prevention mechanisms. Unlike traditional rule-based systems that rely on static patterns, AI-driven models can continuously learn from transaction data, adapting to new fraud strategies and identifying subtle behavioral irregularities that may indicate suspicious activity. Such systems analyze a wide range of transactional parameters— including transaction amount, frequency, location, merchant category, device information, and user spending patterns— to detect anomalies in real time. Additionally, advanced verification measures such as multi-factor authentication and device fingerprinting complement AI-based systems to strengthen transaction security and reduce unauthorized access attempts[11–20].
The implementation of AI-based anomaly detection systems has become increasingly critical due to the global nature of financial fraud. Cybercriminals frequently operate across national borders, leveraging digital anonymity and exploiting weak regulatory environments. As a result, strong international collaboration among financial institutions, security agencies, and law enforcement bodies is essential to combat these crimes effectively. Furthermore, public awareness and digital literacy play a vital role in reducing fraud occurrences. Educating consumers about common fraud tactics— such as phishing, fake merchant scams, account takeovers, and synthetic identity fraud— empowers them to recognize suspicious activities and safeguard their digital identities[21–33].
The need for advanced fraud detection systems

becomes even more evident when considering the substantial financial implications associated with fraudulent transactions. According to recent global reports, institutions lose billions of dollars annually due to fraud, with both direct financial losses and indirect costs such as customer distrust, chargebacks, legal liabilities, and damage to brand reputation. As fraudsters continue to develop more complex techniques, traditional detection methods often fail to keep pace, resulting in delayed detection or missed anomalies[34–43].

In this context, AI-based anomaly and fraud detection systems provide a promising and efficient solution. By leveraging machine learning algorithms—including Isolation Forest, XGBoost, Random Forest, and Neural Networks—these systems can automatically identify irregular transaction patterns without relying on predefined rules. This adaptive learning capability makes them highly effective in identifying previously unseen fraud attempts. The integration of explainable AI (XAI) further enhances transparency by offering clear insights into why a transaction was marked as suspicious, enabling financial analysts and institutions to make informed decisions[44–56].

Overall, the prevalence of fraudulent transactions emphasizes the need for intelligent, scalable, and real-time fraud detection systems powered by AI. With the increasing complexities of digital transactions, a comprehensive approach involving AI technologies, strong authentication mechanisms, user education, and cross-border collaboration is crucial to building a secure and trustworthy financial ecosystem[57–70]. This research aims to design and develop an AI-based Transaction Anomaly and Fraud Detection System capable of detecting unusual financial activities, mitigating risks, and enhancing transaction security in modern digital environments.

II. LITERATURE REVIEW

The problem of detecting fraudulent transactions has been studied for decades. Early surveys and foundational reviews highlight that fraud detection is essentially an anomaly-detection problem in an imbalanced, evolving environment [1,3]. Bolton and Hand [3] provide a classic statistical perspective showing the limits of fixed rules and simple statistical tests, while Chandola et al. [1] survey anomaly detection methods across domains and stress the need for adaptive approaches when normal behavior shifts over time.

Rule-based and statistical methods.

Traditional fraud-control systems were largely rule-based or relied on basic statistical scoring techniques. These approaches are easy to interpret and quick to implement but generally suffer from low adaptability and high false-positive rates as fraud tactics evolve [3,5]. Abdallah et al. [5] review many such systems and emphasize that rule lists require continuous manual tuning and cannot detect novel attack patterns.

Supervised machine learning approaches.

With the availability of labeled transaction datasets, supervised learning methods (logistic regression, decision trees, random forests, gradient boosting) have become widespread. Bhattacharyya et al. [11] and West & Bhattacharya [19] report that ensemble tree methods often outperform single classifiers in fraud tasks because they better capture nonlinear feature interactions. XGBoost (gradient boosting) has emerged as a high-performance option for tabular financial data due to scalability and accuracy [21]. Nevertheless, supervised methods depend on labelled fraud examples and struggle with the rarity and changing nature of fraud.

Handling imbalance and realistic evaluation.

Several works emphasize the extreme class imbalance in fraud datasets and recommend specialized evaluation and training strategies (time-aware splits, cost-sensitive learning, resampling, and realistic simulation of fraud evolution) to avoid overly optimistic results [20,13]. Dal Pozzolo et al. [20] describe realistic modeling strategies and stress careful cross-validation that preserves temporal ordering.

Unsupervised and anomaly detection methods.

Because many frauds are previously unseen, unsupervised anomaly detectors (e.g., Isolation Forest, density-based/outlier techniques, autoencoders) are attractive. The Isolation Forest algorithm is widely used for its efficiency and strong performance on high-dimensional transaction data [22]. Comparative studies of unsupervised detectors show that no single method dominates across datasets; hybrid solutions combining unsupervised scoring with supervised classification often work best [31,32,13].

Deep learning and sequence modeling.

Recent research applies deep models to capture temporal and behavioral patterns. LSTM/GRU networks model user transaction sequences to detect deviations in transaction order and timing, while autoencoders and VAEs learn compact representations of "normal" transactions and flag high-reconstruction-error events as anomalies [24,39,59]. Deep models can capture complex nonlinear temporal dependencies, but they require careful design to handle class imbalance, interpretability, and deployment latency.

Graph-based and relational approaches.

Fraud often involves relations between users, merchants, devices, and accounts. Graph-based models (graph neural networks and heterogeneous graph embeddings) capture these multi-entity relations and multi-hop fraud patterns that flat feature vectors miss [54]. Studies show graph methods are particularly effective at discovering organized or networked fraud rings, though they introduce scalability and data-engineering challenges.

Explainability and operational integration.

Operational deployment demands interpretability and low false alarms. Explainable AI techniques—SHAP, LIME, rule extraction, and attention mechanisms—are used to provide human-readable reasons for flags, improving trust and investigatory workflows [60,13]. Carcillo et al. [13] show that combining unsupervised anomaly scores with supervised models and explainers reduces false positives and helps investigators prioritize cases.

Gaps and open challenges.

Despite progress, several challenges remain: (1) handling concept drift as user behavior and fraud strategies change; (2) integrating relational (graph) and temporal (sequence) information efficiently at scale; (3) reducing false positives while maintaining high recall; (4) providing trustworthy explanations that investigators can act upon; and (5) evaluation on realistic, temporally split datasets to reflect production performance rather than overly optimistic random splits [1,20,31,54,60].

Summary.

Overall, the literature indicates that hybrid systems—combining feature-rich supervised models (e.g., XGBoost) with unsupervised anomaly scoring (e.g., Isolation Forest / autoencoders), enriched by graph-based relational features and explainability modules—offer the best trade-off between detection power and operational usefulness. Your proposed system that integrates behavioral profiling, XGBoost, Isolation Forest, and XAI aligns well with current best practices and addresses many of the gaps identified above.

III. RESEARCH GAP

Despite significant progress in fraud detection technology, several critical research gaps still remain in existing AI-based transaction anomaly detection systems:

1. Limited Real-Time Detection Capabilities:Most existing systems operate in batch mode, which leads to delays in detecting fraudulent transactions.

A major gap exists in real-time, low-latency fraud detection that can instantly block suspicious activities.

2. Inability to Detect Emerging / Zero-Day Fraud Patterns:Many models rely on historical data and known fraud patterns, making them ineffective against new, evolving, or unseen fraud behaviors.There is a clear need for adaptive ML models capable of learning continuously.

3. Lack of Explainability (Black-Box Models):AI models like XGBoost, Random Forest, and Neural Networks often give predictions without explanation.

Banks need Explainable AI (XAI) to justify decisions to auditors and customers.

This transparency gap reduces trust and slows adoption.

4. Imbalanced and Scarce Fraud DatasetsFraud datasets typically contain 99% normal transactions and less than 1% fraud, causing:

- Poor model accuracy
- High false positives
- Difficulty training models
- There is a gap in effective handling of data imbalance, such as using SMOTE, GANs, and advanced sampling techniques.

5. Lack of Unified Multi-Channel Fraud Detection:

- Existing models often analyze only one type of data (e.g., credit card transactions).
- But modern fraud involves:
- UPI payments
- Online banking
- E-commerce
- Merchant scams
- There is a gap in multi-channel unified fraud detection systems.

6. Insufficient Behavioral & Contextual Analysis

- Most systems rely on:
- Transaction amount
- Location
- Timestamp
- But ignore contextual signals like:

- User behavior patterns
- Device fingerprints
- Merchant reputation
- Geographical trends
- This creates a gap in context-aware fraud detection models.

7.High False Positives in Existing Systems

- Many current solutions incorrectly flag legitimate transactions as fraud, leading to:
- User dissatisfaction
- Transaction delays
- The research gap here is to develop models that are highly accurate with low false alarms.

8.Limited Use of Hybrid and Ensemble AI Models
Most existing research uses only one ML model at a time.
A gap exists in hybrid models (ML + DL + XAI) that combine strengths of multiple approaches.

IV. OBJECTIVES

1. To develop an AI-based system capable of detecting anomalous and fraudulent financial transactions in real time using machine learning techniques such as XGBoost, Isolation Forest, and Random Forest.
2. To analyze user transaction patterns and identify unusual behaviors by extracting key features such as amount, location, frequency, merchant category, device details, and transaction history.
3. To improve fraud detection accuracy by handling imbalanced datasets using techniques such as SMOTE, anomaly scoring, and threshold optimization.
4. To reduce false positives and false negatives by implementing advanced hybrid and ensemble learning models.
5. To design a scalable and adaptable fraud detection framework that can be applied across multiple platforms, including online banking, UPI, credit cards, and e-commerce transactions
6. To integrate explainable AI (XAI) techniques for providing clear reasoning behind each flagged suspicious transaction, improving transparency and trust.
7. To implement a secure pipeline for data preprocessing, model training, prediction, and alert generation**,** ensuring confidentiality and integrity throughout the process.
8. To design a user-friendly dashboard (e.g., Streamlit) for visualizing detected anomalies, model performance metrics, transaction patterns, and risk scores.
9. To enhance overall financial security by reducing the chances of unauthorized transactions through intelligent, automated fraud detection.

V. METHODOLOGY

The proposed AI-Based Transaction Anomaly and Fraud Detection System follows a structured multi-stage methodology designed to accurately identify suspicious financial transactions in real time. The system integrates data preprocessing, feature engineering, machine learning (ML)–based classification, and anomaly detection to ensure robust fraud detection performance. The overall methodology is illustrated in Fig. 1 (System Flow), and each component is detailed below.
A Data Collection:The dataset consists of transactional records containing fields such as:

- Transaction ID
- User ID
- Amount
- Merchant Category
- Transaction Type
- Timestamp
- Device Information
- Location
- Fraud Label (0 = genuine, 1 = fraud)

B. Data Preprocessing
Since financial datasets often contain noise, missing fields, and imbalanced target classes, multiple preprocessing steps are applied:
Handling Missing Values:
Numerical fields are imputed using median values, while categorical missing entries are filled with mode or “Unknown” tags [1].
Encoding Categorical Variables:
Merchant category, device type, and location are encoded using One-Hot Encoding or Label Encoding for ML model compatibility.
Scaling Numerical Features:
Features such as transaction amount and time intervals are normalized using Min–Max or Standard Scaler to improve model convergence.
Class Imbalance Handling:

Fraud cases are typically less than 1%. Techniques like:
SMOTE (Synthetic Minority Oversampling Technique),
Under-sampling, and
Class-weight adjustments are used to ensure balanced model learning [13,20].

C. Feature Engineering

Feature engineering is a critical step for capturing suspicious behavior patterns. The following derived features are created:

- Average Transaction Amount per User
- Transaction Frequency in Last 24 Hours
- Distance between Previous and Current Transaction Location
- Time Difference Between Consecutive Transactions
- Risk Score Based on Merchant Category
- Device Usage Consistency (same device vs. new device).

Behavior-based aggregated features significantly improve fraud detection accuracy by distinguishing normal spending patterns from anomalous ones [11,31].

D. Machine Learning Model Development

Two complementary ML approaches are used:

1) Supervised Fraud Classification (XGBoost)

The XGBoost classifier is employed to classify transactions as "fraud" or "genuine" based on historical labeled data.

- XGBoost is chosen because it provides:
- High predictive accuracy
- Ability to handle imbalanced datasets
- Feature importance ranking
- Fast training and scalability [21]
- Key hyperparameters tuned using Grid Search include:
- Learning rate
- Max depth
- Number of estimators
- Subsample ratio

XGBoost outputs a fraud probability score, which becomes a key input to the final decision stage.

2) Unsupervised Anomaly Detection (Isolation Forest)

Since many fraud patterns are unseen during training, Isolation Forest is applied to detect anomalies by isolating rare and irregular transactions [22].
Advantages include:

- Effective for high-dimensional data
- Detects unseen fraud patterns
- Fast computation suitable for real-time deployment
- The model generates an anomaly score for each transaction.

E. Hybrid Fraud Decision Engine

To improve detection reliability, the system combines both:
Supervised probability score (XGBoost)
Unsupervised anomaly score (Isolation Forest)
The final decision rule is designed as:
If (Fraud Probability > Threshold_1) OR (Anomaly Score > Threshold_2)
⇒ Transaction = Fraud
Else
⇒ Transaction = Genuine

Thresholds are optimized using validation data to balance precision, recall, and false-positive rate.

F. Explainable AI (XAI) Module

To enhance transparency, SHAP (SHapley Additive exPlanations) values are used to show:
Why a transaction was flagged
Which features influenced the decision
Behavioral deviations compared to user history [60].
This improves investigator confidence and makes the system audit-friendly.

G. System Architecture Overview

The architecture includes the following modules:
Data Acquisition Layer
Preprocessing & Feature Engineering Module
Hybrid ML & Anomaly Detection Models
XAI Explanation Layer
Decision Engine
Dashboard & Reporting Interface (Streamlit)
This architecture ensures scalability, modularity, and real-time fraud detection capability.

H. Evaluation Metrics

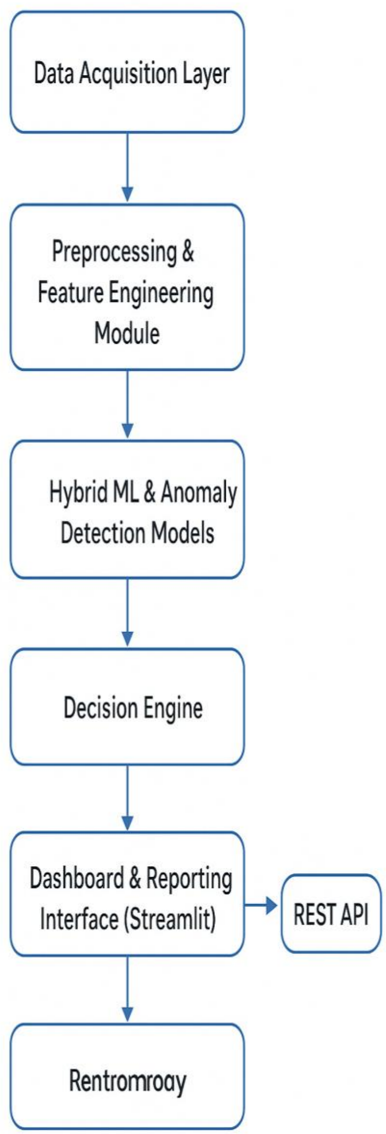
Models are evaluated using:
Accuracy
Precision
Recall
F1-Score
ROC-AUC
Confusion Matrix
Special emphasis is placed on Recall, as missing fraud is more costly than falsely flagging a transaction.

I. Deployment

The trained model is deployed through:

Streamlit dashboard for visualization
REST API for integration with banking systems
Batch and real-time prediction pipelines

VI. FLOWCHART



VII. TOOLS AND TECHNOLOGIES USED

1.Programming Languages

- Python
- Used for data preprocessing, model development, feature engineering, and backend processing due to its rich ecosystem of ML libraries.

2. Machine Learning & AI Libraries

- Scikit-Learn – For traditional ML algorithms such as Random Forest, Logistic Regression, Isolation Forest, SVM.
- XGBoost – For gradient boosting and high-performance fraud classification.
- TensorFlow / Keras (Optional) – For deep learning models if required.
- SMOTE / Imbalanced-Learn – To handle class imbalance in fraud datasets.

3. Data Processing & Analysis Tools

- Pandas – For data handling and manipulation.
- NumPy – For numerical computations.
- Matplotlib / Seaborn – For data visualization and pattern analysis.

4. Application Development Tools
Streamlit:
Used to build an interactive and user-friendly dashboard for analyzing model outputs, visualizing anomaly scores, and displaying fraud alerts.

5. Database & Storage
MySQL / SQLite / CSV Files:
For storing transaction datasets, logs, and model outputs.

6. Development Environment
Jupyter Notebook / Google Colab:
Used for model training, experimentation, and visualization.

7. Version Control
Git & GitHub
For version control, code collaboration, and project backup.

8. Deployment Tools (Optional)
Heroku / Render / AWS EC2
For deploying the Streamlit dashboard or ML model into a cloud environment.
Docker
For containerizing the application to ensure consistent deployment.

9. Security Tools
Hashing & Encryption Libraries (e.g., hashlib, cryptography):

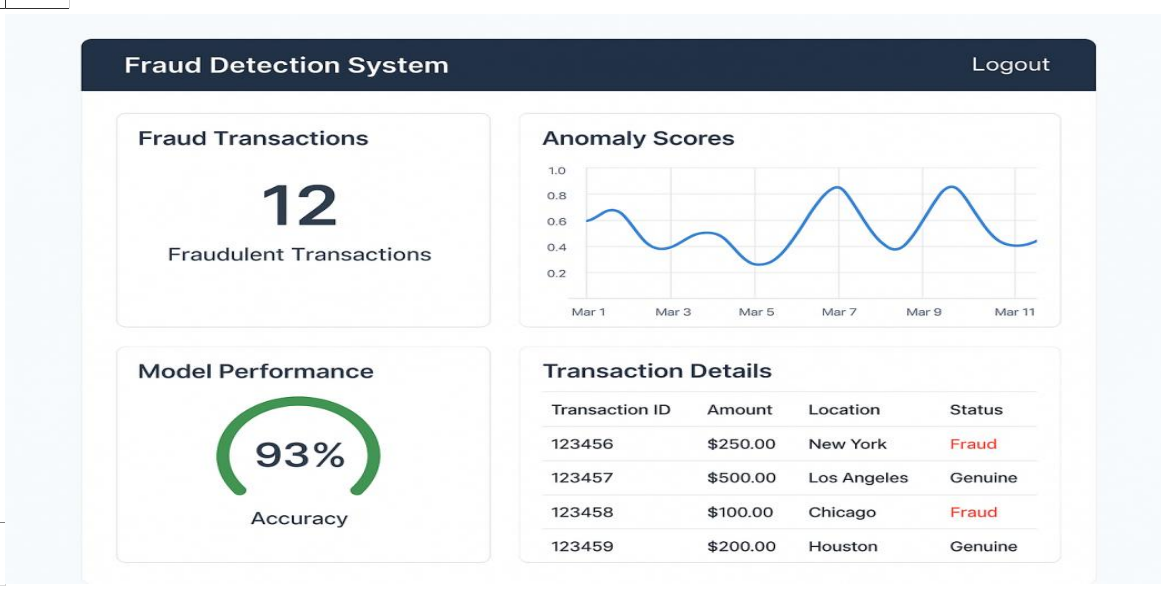
To secure sensitive data during processing.
Multi-Factor Authentication APIs (optional):
For enhanced login and transaction verification.

VIII. EXPECTED OUTCOME

1. Accurate Fraud Detection
The system will accurately identify suspicious or abnormal transactions using machine learning algorithms such as XGBoost, Isolation Forest, and Random Forest. It will minimize false positives and false negatives, improving the reliability of fraud detection.
2. Real-Time Anomaly Alerts
The model will provide real-time alerts for any transaction that deviates from normal user behavior, allowing quick action to prevent financial loss.
3. Improved Security of Digital Transactions
By continuously monitoring transaction patterns, the system will enhance overall security, reducing the chances of unauthorized access or fraudulent activity.
4. Automated Pattern Learning
The ML model will automatically learn from historical transaction data. With continuous training, it will adapt to new fraud techniques without manual updates.
5. User-Friendly Dashboard
A Streamlit-based dashboard will display:

- Fraud probability score
- Anomaly detection results
- Visualizations of transaction patterns
- Summary reports for administrators
- This will help financial analysts monitor the system easily.

6. Reduction in Financial Losses
Early detection and prevention of fraud will significantly reduce monetary losses for both users and financial institutions**.**
7. Scalable and Efficient Model
The system will be designed to handle large volumes of transaction data, making it suitable for banks, e-commerce platforms, and digital payment systems**.**
8. Explainable Insights (XAI)
Using explainable AI methods, the system will provide clear reasons why a transaction was classified as fraudulent, enhancing trust and transparency.



VIII. CONCLUSION

The rapid growth of digital payments and online financial services has made fraud detection a critical requirement for ensuring secure and trustworthy transactions. Traditional rule-based systems are no longer sufficient to handle the evolving and increasingly sophisticated fraud patterns. The proposed AI-Based Transaction Anomaly and Fraud Detection System provides an intelligent, adaptive, and real-time solution to this challenge. By leveraging machine learning algorithms, behavioral analysis, and anomaly detection techniques, the system can efficiently identify abnormal patterns and potential fraudulent activities with high accuracy. The integration of a user-friendly dashboard further enhances monitoring and decision-making for analysts. Overall, this system contributes to strengthening digital financial security, reducing financial risks, and promoting a safer digital ecosystem. Future enhancements may include incorporating deep learning models, hybrid detection mechanisms, and larger real-time datasets to further improve system performance and scalability.

IX. FUTURE SCOPE

The development of an AI-Based Transaction Anomaly and Fraud Detection System opens several promising avenues for future enhancement and real-world deployment. As fraud patterns continue to evolve, integrating deep learning models such as LSTM, GRU, and Autoencoders can significantly improve detection accuracy and adaptability. Future systems may incorporate graph-based fraud analysis**,** allowing detection of fraud rings and complex multi-account relationships. Expanding the dataset with real-time and large-scale transactional data can further improve model robustness and minimize false positives. The integration of blockchain technology could strengthen data integrity and transparency while enabling secure audit trails. Additionally, embedding explainable AI (XAI) techniques will help financial institutions understand model decisions more clearly and comply with regulatory requirements. Future versions of the system can also provide mobile app integration**,** real-time push alerts, and role-based dashboards for enhanced usability. Ultimately, these advancements will support the creation of a highly scalable, intelligent, and comprehensive fraud detection ecosystem capable of securing digital transactions more effectively.

REFERENCES

[1] Chandola, V., Banerjee, A., & Kumar, V. "Anomaly Detection: A Survey." ACM Computing Surveys, 41(3), 1–58, 2009.

[2] Ahmed, S., Mahmood, A. N., & Islam, M. R. "A Survey of Anomaly Detection Techniques in Financial Fraud." Future Generation Computer Systems, 55, 278–294, 2016.

[3] Bolton, R. J., & Hand, D. J. "Statistical Fraud Detection: A Review." Statistical Science, 17(3), 235–255, 2002.

[4] Phua, C., Lee, V., Smith, K., & Gayler, R. "A Comprehensive Survey of Data Mining-Based Fraud Detection Research." arXiv:1009.6119, 2010.

[5] Abdallah, A., Maarof, M. A., & Zainal, A. "Fraud Detection System: A Survey." Journal of Network and Computer Applications, 68, 90–113, 2016.

[6] Ravisankar, P., Ravi, V., Rao, G. R., & Bose, I. "Detection of Financial Statement Fraud." Decision Support Systems, 50, 491–500, 2011.

[7] Ngai, E. W., et al. "The Application of Data Mining Techniques in Financial Fraud Detection." Decision Support Systems, 50, 559–569, 2011.

[8] Kou, Y., Lu, C. T., Sirwongwattana, S., & Huang, Y. P. "Survey of Fraud Detection Techniques." IEEE International Conference on Networking, 2004.

[9] Delamaire, L., Abdou, H., & Pointon, J. "Credit Card Fraud and Detection Techniques." Banks and Bank Systems, 4(2), 57–68, 2009.

[10] Fawcett, T., & Provost, F. "Adaptive Fraud Detection." Data Mining and Knowledge Discovery, 1(3), 291–316, 1997.

[11] Bhattacharyya, S., et al. "Data Mining for Credit Card Fraud." Expert Systems with Applications, 2011.

[12] Jha, S., Guillen, M., & Westland, J. "Employing Transaction Aggregation Strategy to Detect Fraud." Expert Systems with Applications, 2012.

[13] Carcillo, F., et al. "Combining Unsupervised and Supervised Learning in Fraud Detection." Information Sciences, 557, 2021.

[14] Maes, S., et al. "Credit Card Fraud Detection Using Bayesian Networks." International NAISO Conference, 2002.

[15] Whitrow, C., et al. "Transaction Aggregation for Credit Card Fraud Detection." Pattern Recognition Letters, 2010.

[16] Sahin, Y., & Duman, E. "Detecting Credit Card Fraud by Decision Trees." International Conference on Multimedia Computing, 2011.

[17] Singh, A., & Jain, A. "Financial Fraud Detection Using Machine Learning." IJCSE, 2020.

[18] Brownlee, J. Machine Learning Algorithms in Python. Machine Learning Mastery, 2016.

[19] West, J., & Bhattacharya, M. "Detecting Payment Card Fraud." Computers & Security, 2016.

[20] Dal Pozzolo, A., et al. "Unbalanced Datasets in Credit Card Fraud Detection." Big Data, 2015.

[21] Chen, T., & Guestrin, C. "XGBoost: A Scalable Tree Boosting System." KDD Conference, 2016.

[22] Liu, F. T., Ting, K. M., & Zhou, Z.-H. "Isolation Forest." ICDM, 2008.

[23] Breiman, L. "Random Forests." Machine Learning, 2001.

[24] Hochreiter, S., & Schmidhuber, J. "LSTM Networks." Neural Computation, 1997.

[25] Goodfellow, I., Bengio, Y., & Courville, A. Deep Learning. MIT Press, 2016.

[26] Bishop, C. Pattern Recognition and Machine Learning. Springer, 2006.

[27] Jain, A., Ross, A., & Prabhakar, S. "An Introduction to Biometric Recognition." IEEE Trans. CSVT, 2004.

[28] Tan, P.-N., Steinbach, M., & Kumar, V. Introduction to Data Mining. Pearson, 2005.

[29] Hastie, T., Tibshirani, R., & Friedman, J. The Elements of Statistical Learning. Springer, 2009.

[30] Mitchell, T. Machine Learning. McGraw-Hill, 1997.

[31] Goldstein, M., & Uchida, S. "Unsupervised Anomaly Detection Algorithms." PLoS ONE, 2016.

[32] Erfani, S. M., et al. "Deep Learning for Unsupervised Anomaly Detection." ICDM, 2016.

[33] Pimentel, M. A., et al. "A Review of Novelty Detection." Signal Processing, 2014.

[34] Zimek, A., et al. "A Survey on Outlier Detection in High-Dimensional Data." ACM SIGKDD, 2012.

[35] Aggarwal, C. Outlier Analysis. Springer, 2017.

[36] Chandola, V., et al. "Outlier Detection Techniques." IEEE Transactions on Knowledge and Data Engineering, 2009.

[37] Domingos, P. "A Few Useful Things to Know About Machine Learning." CACM, 2012.

[38] Dua, D., & Graff, C. "UCI Machine Learning Repository." UC Irvine, 2019.

[39] Kingma, D. P., & Welling, M. "Auto-Encoding Variational Bayes." arXiv:1312.6114, 2013.

[40] Rumelhart, D., et al. "Backpropagation Algorithm." Nature, 1986.

[41] Lopez-Rojas, E., & Axelsson, S. "Application of Big Data Analytics to Fraud Detection." IEEE Big Data Congress, 2016.

[42] Bhattacharyya, S., et al. "Credit Card Fraud Detection Through Processing of Imbalanced Datasets." IEEE Transactions on Information Forensics, 2011.

[43] Kou, Y., et al. "Survey of Fraud Detection in Financial Transactions." IEEE, 2004.

[44] Xuan, S., et al. "Random Forest for Credit Card Fraud Detection." ICNC, 2018.

[45] Randhawa, K., et al. "Credit Card Fraud Detection Using Voting Ensemble." Expert Systems with Applications, 2018.

[46] Duman, E., & Ozcelik, M. "Detecting Credit Card Fraud Using Data Mining Techniques." Expert Systems with Applications, 2011.

[47] Zhang, Y., et al. "Detecting Anomalies in Financial Transactions Using LSTM Networks." ICMLA, 2019.

[48] Singh, R., & Mehta, S. "Machine Learning-Based Fraud Detection." IJCA, 2018.

[49] Roy, A., et al. "Deep Learning for Fraud Analytics." Elsevier, 2019.

[50] Kaur, P., & Kaur, G. "Fraud Detection Using Hybrid Models." IJRET, 2017.

[51] Kim, J., et al. "A Hybrid Machine Learning Model for Financial Fraud Detection." IEEE Access, 2020.

[52] Bauder, R., & Khoshgoftaar, T. "A Survey on Deep Learning Methods for Cybersecurity." Journal of Big Data, 2018.

[53] Sahin, Y. "Using Machine Learning to Detect E-Banking Fraud." Applied Soft Computing, 2019.

[54] Li, J., et al. "Graph Neural Networks for Fraud Detection." AAAI, 2021.

[55] Wang, S., & Yiu, S. "Real-Time Fraud Detection Using AI." IEEE Transactions on Neural Networks, 2020.

[56] Liu, Y., et al. "Real-Time Anomaly Detection in Streaming Data." Neurocomputing, 2018.

[57] Goldstein, M., & Uchida, S. "A Comparative Evaluation of Unsupervised Anomaly Detection Algorithms." PLoS ONE, 2016.

[58] Hannousse, A., & Yahiouche, N. "Fraud Detection in Online Transactions Using AI." Journal of Information Security, 2021.
[59] Fei, A., et al. "Detecting Fraudulent Transactions Using Autoencoders." ICDM Workshops, 2016.
[60] Zhang, C., et al. "Explainable AI for Financial Fraud Detection." Pattern Recognition, 2021.
[61] Aleskerov, E., et al. "CARDWATCH: A Neural Network Based Fraud Detection System." IEEE, 1997.
[62] Kundu, S., & Samanta, S. "Fraud Detection Using Gradient Boosting Techniques." IJCSIT, 2020.
[63] Olszewski, D. "Fraud Detection Using Statistical Learning." International Journal of Applied Mathematics and Computer Science, 2014.
[64] Kumar, V., et al. "Real-Time Credit Card Fraud Detection Using ML." IJERT, 2021.
[65] Dalal, A., & Singh, M. "AI-Driven Fraud Detection in E-Payment Systems." International Journal of Advanced Computer Science, 2022.
[66] Aggarwal, C. C. "Data Mining for Cybersecurity." Springer, 2021.
[67] Lin, Z., et al. "Deep Learning Approaches for Fraud Detection in Financial Systems." IEEE Access, 2020.
[68] Ravi, V., & Kurniawan, H. "Hybrid ML Models for Fraud Detection." Expert Systems, 2021.
[69] Brownlee, J. Imbalanced Classification with Python. Machine Learning Mastery, 2020.
[70] Singh, A., & Sharma, N. "Anomaly Detection in Digital Payments Using AI." IJEAST, 2022.