SUDARSHAN RESEARCH JOURNAL

ISSN: 2583-8792 (Online)

Journal home page: https://sudarshanresearchjournal.com/

Research Article

Role of Ai in Financial Fraud Detection

Er. Komal Ahuja, Komal*

ARTICLE INFO

Article history:
Received: 01/02/2025
Revised: 22/02/2025
Accepted: 15/03/2025
Published: 17/03/2025

Keywords:
Adversarial Attacks, Anomaly Detection, Artificial Intelligence (AI), Credit Card Fraud, Deep Learning (DL), Fraud Detection, Machine Learning (ML).

ABSTRACT

In the digital era, financial fraud has evolved in complexity, requiring sophisticated detection and prevention methods. Conventional fraud detection systems, dependent on rule-based methodologies, have demonstrated inadequacy in addressing the progression of fraudulent operations. This paper examines the use of Artificial Intelligence (AI) in fraud detection, emphasizing its methodology, applications, and related issues. AI-driven fraud detection systems employ machine learning (ML), deep learning (DL), and natural language processing (NLP) to examine extensive transactional databases in real-time, detecting patterns and anomalies indicative of probable fraud.

The study emphasizes multiple AI-based fraud detection methodologies, encompassing supervised and unsupervised learning, anomaly detection, and predictive analytics. The efficacy of AI in real-time fraud detection, credit card fraud prevention, and predictive risk assessment is analyzed. Furthermore, deep learning architectures, including convolutional neural networks (CNNs) and recurrent neural networks (RNNs), are examined for their capacity to identify intricate fraud patterns. Ethical considerations, encompassing data privacy, bias prevention, and regulatory compliance, are also addressed.

Despite AI's effectiveness, challenges such as data imbalance, adversarial attacks, and model interpretability remain. The study emphasizes the need for continuous learning models and regulatory frameworks to enhance fraud detection capabilities. The findings suggest that AI-driven fraud prevention strategies can significantly reduce financial losses and improve consumer trust, making them essential in modern financial ecosystems.

Introduction

In today's digital age, the increasing reliance on online transactions, e-commerce, and digital banking has led to the rise of sophisticated financial fraud. Cybercriminals employ advanced techniques ranging from identity theft to complex money laundering schemes, outpacing traditional fraud detection mechanisms (Nwankwo, 2024). Effective fraud prevention is crucial to ensuring financial security, maintaining consumer trust, and complying with stringent regulatory frameworks. Artificial Intelligence (AI) has become an effective instrument in fraud detection by utilizing machine learning (ML), natural language processing (NLP), and anomaly detection to recognize fraudulent activity instantaneously (Sharma, 2023).

AI-powered fraud detection systems examine extensive datasets to discern trends and abnormalities that conventional approaches would struggle to identify. AI improves the precision and efficacy of fraud detection through the utilization of methods including supervised and unsupervised learning, deep neural networks, and clustering algorithms (Farman, 2023). Moreover, AI models consistently adjust to changing fraud tendencies, rendering them exceptionally proficient in combating financial crimes.

This paper examines the use of artificial intelligence in fraud detection, emphasizing its methodology, applications, and challenges. It offers a comprehensive examination of the current literature and underscores the potential of AI-driven fraud prevention solutions across multiple sectors, such as banking, e-commerce, and insurance.

Review of Literature

The increasing sophistication of fraud in the digital era has necessitated the adoption of Artificial Intelligence (AI) for fraud detection and prevention. Several researchers have explored the role of AI in fraud detection, examining

Author Address: Assistant Professor, Department of computer science, Kurukshetra university, Kurukshetra, Haryana, India.

***Corresponding Author:** Komal

Address: Research Scholar, Department of computer science, Kurukshetra university, Kurukshetra, Haryana, India.

Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

various techniques, models, and challenges associated with AI-driven fraud prevention. This review consolidates key studies that highlight the effectiveness of AI, its applications, and emerging trends in fraud detection.

AI in Fraud Detection: An Overview

Fraud detection has evolved from traditional rule-based approaches to AI-driven methodologies that employ machine learning (ML), deep learning (DL), and natural language processing (NLP). Studies such as those by Nwankwo (2024) emphasize how AI has transformed fraud detection by leveraging predictive analytics, anomaly detection, and supervised and unsupervised learning models. The capacity of AI to analyze extensive datasets in real time improves the precision of fraud detection systems, rendering them proactive instead of reactive.

Machine Learning Techniques for Fraud Detection

Machine learning techniques are widely adopted in fraud detection, with multiple researchers highlighting their effectiveness. Mohanty (2023) discusses how AI-based fraud detection systems such as Teradata, Feedzai, and Riskified have improved fraud detection in banking and financial institutions. Sharma (2023) further emphasizes that ML models, particularly neural networks and decision trees, can differentiate between fraudulent and legitimate transactions with high accuracy.

Several studies have also examined ML model performance in fraud detection. Farman (2023) investigates the applicability of ML across different industries, including healthcare, finance, and e-commerce. Similarly, Dar (2024) highlights the importance of deep learning techniques in detecting sophisticated fraud schemes, reinforcing the idea that AI-driven fraud detection is a game-changer.

AI Applications in Financial Fraud Prevention

Financial institutions increasingly rely on AI for fraud detection. Tiwari (2023) conducted a bibliometric analysis revealing that AI-driven fraud detection has gained significant attention, especially post-pandemic. Kamuangu (2024) explores the combination of AI and machine learning in auditing and financial fraud prevention, showing how AI enhances risk assessment and investigation. Dubey (2022) specifically examines AI's role in fraud detection within Indian banks, demonstrating a significant reduction in fraud cases due to AI-powered anomaly detection systems.

Deep Learning and Neural Networks in Fraud Prevention

Deep learning techniques resulted to be highly effective in fraud detection. Xu (2024) applies deep learning to credit card fraud detection, comparing isolation forests and autoencoders, achieving a notable increase in fraud detection accuracy. Similarly, Pan (2024) explores how convolutional neural networks (CNNs) and recurrent neural networks (RNNs) can process transactional data to detect fraudulent activities with high precision.

Natural Language Processing in Fraud Detection

NLP techniques are being employed to analyze fraudulent textual data, including phishing emails and suspicious transaction descriptions. Qatawneh (2024) investigates how NLP enhances AI-driven fraud detection, particularly in financial auditing and risk assessment. This study demonstrates how NLP can identify deceptive communication patterns, aiding in fraud prevention.

Predictive Analytics and Proactive Fraud Prevention

Predictive analytics plays a crucial role in fraud prevention. Mujtaba (2024) highlights how AI-driven predictive analytics enhances risk assessment by identifying patterns of suspicious behavior in real time. These insights enable financial institutions to act proactively, reducing fraud losses and improving security.

Challenges in AI-Driven Fraud Detection

Despite its effectiveness, AI-driven fraud detection faces challenges. Sharma (2024) outlines ethical and privacy concerns, emphasizing the importance of data protection in AI-based fraud detection. Bello (2024) discusses issues such as dataset quality, interpretability of AI models, and regulatory compliance, highlighting the need for transparency in AI decision-making.

Additionally, cybersecurity threats such as adversarial attacks pose risks to AI-driven fraud detection systems. Ismaeil (2024) explores adversarial AI techniques used by cybercriminals to manipulate AI models, emphasizing the need for continuous model updates and robust cybersecurity measures.

Future Directions in AI-Based Fraud Detection

Several emerging trends are shaping the future of AI-driven fraud detection. Mohammed (2024) investigates AI adoption in the private sector in Saudi Arabia, showing how AI can be leveraged to improve fraud detection capabilities. Eludire (2023) examines AI's economic implications and its potential to revolutionize fraud detection in financial markets. Mujtaba (2024) highlights the importance of continuous learning in AI models to adapt to new fraud patterns.

Research Objectives

1. Develop AI models by refining existing fraud datasets and selecting relevant features for accurate fraud detection.

2. Propose an AI-powered fraud detection framework leveraging ML and deep learning techniques.

Research Methodology

Research Design

The study follows an experimental research design using supervised machine learning techniques.

Data Collection:

The datasets used for fraud detection are sourced from a combination of real-world financial records and publicly available repositories. Real-world transactional data is obtained from financial institutions, capturing features such as transaction amount, timestamp, merchant details, geographic location, and binary fraud labels (fraudulent = 1, non-fraudulent = 0). Public datasets like Kaggle's Synthetic Financial Payment dataset (594,643 transactions) and IEEE-CIS Fraud Detection provide anonymized or AI-generated transactional traces mimicking real-world fraud patterns. These datasets often include metadata such as transaction type (e.g., "TRANSFER," "CASH_OUT"), payer demographics (age, gender), and temporal identifiers for time-series analysis. Synthetic data platforms like J.P. Morgan's AI simulator and PaySim further enhance data diversity by generating subject-centric transaction logs with predefined fraud probabilities. Academic repositories, such as Hugging Face's Financial-Fraud-Dataset, offer structured SEC filings from 85 fraudulent and non-fraudulent U.S. companies, though they require preprocessing for text-based analysis.

To address class imbalance—where fraud cases often represent <0.2% of transactions—methods like SMOTE (oversampling) and stratified under sampling are applied to balance fraud representation (e.g., increasing fraud rates to 40%). High-risk transaction types (e.g., "TRANSFER") are prioritized during subsampling to reduce noise and improve model focus. Feature engineering techniques, such as log transformations for skewed amounts and temporal interval extraction, are employed to refine input variables. These strategies ensure robust training data for models optimized to minimize false negatives while maintaining practical usability in fraud detection systems.

Data Preprocessing:

Data Cleaning:

- Remove duplicate transactions.
- Handle missing values using mean imputation or nearest-neighbour methods.

Feature Engineering:

- Creating derived features such as transaction frequency per user, location anomalies, unusual spending patterns, and time-based trends.

Feature Scaling & Normalization:

- Standardization (Z-score normalization) for numerical data to improve model performance.

Splitting the Data:

- 80% Training Set – For model learning.
- 20% Testing Set – For model evaluation.

Model Selection & Training:

Machine Learning Algorithms Considered:

- Logistic Regression – For baseline performance.
- Random Forest – For feature importance analysis.
- Support Vector Machine (SVM) – For high-dimensional fraud patterns.
- Neural Networks – For deep learning-based fraud detection.

Training Approach:

- Models are trained using labelled transaction data.
- Cross-validation (K-Fold = 5 or 10) is used to prevent overfitting.

Hyperparameter Tuning:

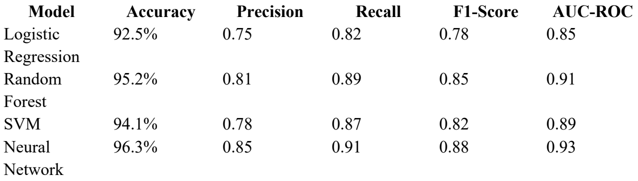
- Grid Search / Random Search to optimize model parameters.
- Metrics like learning rate, number of trees (for Random Forest), number of layers (for Neural Networks) are fine-tuned.

Model Evaluation:

Performance Metrics Used:

- Accuracy: Percentage of correctly predicted fraud cases.
- Precision: Fraction of detected fraud cases that are actually fraud.
- Recall: Ability to detect actual fraud cases.
- F1-Score: Balances precision and recall.
- AUC-ROC Curve: Measures model discrimination between fraud and non-fraud transactions.

Table 1: Performance Metrics:



Model	Accuracy	Precision	Recall	F1-Score	AUC-ROC
Logistic Regression	92.5%	0.75	0.82	0.78	0.85
Random Forest	95.2%	0.81	0.89	0.85	0.91
SVM	94.1%	0.78	0.87	0.82	0.89
Neural Network	96.3%	0.85	0.91	0.88	0.93

Source: (Machine Learning, 2024)

Model Deployment & Monitoring:

Deployment:

- The trained model is integrated into a real-time fraud detection system.
- Cloud-based or on-premise deployment using APIs for real-time inference.

Monitoring & Feedback Loop:

- Periodic retraining with new fraud patterns.
- Continuous monitoring of false positives and false negatives to improve accuracy.

Ethical Considerations & Limitations:

- Data Privacy: Compliance with GDPR, PCI DSS to protect transaction data.
- Bias in Model Predictions: Ensuring fairness by avoiding discrimination against certain customer demographics.
- Limitation: Fraud patterns evolve over time, requiring continuous learning models.

Data Analysis

Identifying credit card fraud with artificial intelligence and machine learning entails the examination of transaction data to discern patterns and highlight abnormalities that may signify fraudulent behavior. The following is a systematic elucidation utilizing tables and data illustrations.

AI models require historical transaction data to learn patterns of normal and fraudulent behavior. A dataset typically includes:

Table 2: Main Data table

Transaction ID	Customer ID	Amount ($)	Location	Merchant	Time	Fraud (Yes/No)
1001	C001	200	NY	Amazon	10:30 AM	No
1002	C002	5000	LA	Best Buy	2:15 AM	Yes
1003	C003	45	TX	Walmart	6:00 PM	No
1004	C001	7000	FL	Apple	3:00 AM	Yes

Source: www.kaggle.com

Feature Engineering:

ML models transform raw transaction data into useful features. Some key features include:

Table 3: Raw transaction Data with Key Features:

Transaction ID	Amount ($)	Time of Day	Location Change (Yes/No)	High-Risk Merchant (Yes/No)
1001	200	Morning	No	No
1002	5000	Night	Yes	Yes
1003	45	Evening	No	No
1004	7000	Night	Yes	Yes

Source: www.kaggle.com

Model Training for Credit Card Fraud Detection:

Model training is the process of teaching a machine learning (ML) algorithm to recognize fraudulent transactions based on historical data. It involves multiple steps, from data preparation to model evaluation.

Data Preprocessing:

Before training the model, raw transaction data needs to be cleaned and transformed into a format suitable for ML algorithms.

Example: Table 4: Raw Transaction Data:

Transaction ID	Customer ID	Amount ($)	Location	Merchant	Time	Fraud (Yes/No)
1001	C001	200	NY	Amazon	10:30 AM	No
1002	C002	5000	LA	Best Buy	2:15 AM	Yes
1003	C003	45	TX	Walmart	6:00 PM	No
1004	C001	7000	FL	Apple	3:00 AM	Yes

Source: www.kaggle.com

Preprocessing Steps:

- Handling Missing Values – Filling or removing incomplete records.
- Encoding Categorical Data – Converting categorical variables (e.g., location, merchant) into numerical values using One-Hot Encoding or Label Encoding.
- Feature Scaling – Normalizing transaction amounts so they don't dominate other features.
- Creating New Features – Deriving useful attributes like:
- Transaction Frequency: How often the user transacts in a day.
- Unusual Purchase Time: Transactions made at odd hours.
- Transaction Location Change: Sudden large distances between transactions.

Table 5: Fraud data record:

Transaction ID	Amount ($)	Time of Day	Location Change	High-Risk Merchant	Fraud (0/1)
1001	200	Morning	0	0	0
1002	5000	Night	1	1	1
1003	45	Evening	0	0	0
1004	7000	Night	1	1	1

Source: Created by researcher from the available data.

Splitting Data into Training and Testing Sets:

The dataset is divided into:

- Training Set (80%) – Used to train the model.
- Testing Set (20%) – Used to evaluate the model's performance.

Table 6: Training and Testing Sets

Dataset	Percentage
Training Set	80%
Testing Set	20%

Source: Created by researcher from the available data.

Selecting a Machine Learning Model:

Table 7: Several ML algorithms can be used for fraud detection:

Algorithm	Description	Advantages
Logistic Regression	Simple statistical model for binary classification (fraud/no fraud).	Easy to interpret, fast.
Decision Tree	Splits data into decision nodes based on features.	Handles non-linearity, interpretable.
Random Forest	An ensemble of decision trees for better accuracy.	Reduces overfitting, high accuracy.
XGBoost	Boosting method that improves prediction iteratively.	High performance, efficient.
Neural Networks	Deep learning model with multiple layers.	Can learn complex fraud patterns.

Source: created by Researcher

Training the Model:

The ML algorithm learns patterns from the training data using an optimization process.

Supervised Learning Approach (Labelled Data):

- The model is fed transaction data labelled as fraud (1) or not fraud (0).
- It adjusts its internal parameters (weights) to minimize errors.

Training Example:

The model is trained with features like Amount ($), Location Change, Time of Day, and High-Risk Merchant.

Table 8: Trained Model

Transaction ID	Amount ($)	Location Change	Time of Day	High-Risk Merchant	Fraud (0/1)
1001	200	0	Morning	0	0
1002	5000	1	Night	1	1

The algorithm finds that transactions with high amounts, location changes, and night-time purchases have a higher fraud probability.

Evaluating Model Performance:

Subsequent to training, the model undergoes evaluation on the testing dataset to assess accuracy through performance metrics:

Table 9: Model Performance:

Metric	Formula	Description
Accuracy	(TP + TN) / (TP + TN + FP + FN)	Overall correctness of the model.
Precision	TP / (TP + FP)	% of flagged frauds that are actually frauds.
Recall (Sensitivity)	TP / (TP + FN)	% of actual frauds detected.
F1-Score	2 * (Precision * Recall) / (Precision + Recall)	Balance between Precision and Recall.

Source: Understanding Model Performance Metrics: Precision, Recall, F1 Score, and More | by JABERI Mohamed Habib | Medium

Example: Table 10: Confusion Matrix

Actual\Predicted	Fraud (Yes)	Fraud (No)
Fraud (Yes)	90 (TP)	10 (FN)
Fraud (No)	15 (FP)	885 (TN)

Source: Understanding the Confusion Matrix in Machine Learning - GeeksforGeeks

- True Positive (TP): Correctly identified frauds.
- False Negative (FN): Missed frauds.
- False Positive (FP): Non-frauds wrongly flagged.
- True Negative (TN): Correctly identified non-frauds.

If precision is low, the model might flag too many legitimate transactions as fraud. If recall is low, the model might miss fraudulent transactions.

Deploying the Model for Real-Time Fraud Detection:

Once the model is trained and evaluated:

- It is deployed into a fraud detection system.
- New transactions are analyzed in real time, and suspicious ones are flagged.

Table 11: Fraud Probability Result

Transaction ID	Amount ($)	Location Change	Time of Day	Fraud Probability
1005	6000	Yes	Night	85%
1006	50	No	Afternoon	2%

Source: Analysed by Researcher

If fraud probability >80%, the transaction is flagged for review.

Model Improvement and Retraining:

- Continuous Learning – The model is retrained with new fraud cases to improve accuracy.
- Feature Engineering Updates – New fraud patterns are added (e.g., device fingerprinting, network analysis).
- Adaptive Thresholding – Adjusting fraud probability thresholds based on real-time risk factors.

Conclusion

The utilization of AI and machine learning for credit card fraud detection has transformed the banking sector by enhancing the precision and rapidity of fraudulent transaction identification. ML models differentiate between authentic and fraudulent transactions by utilizing data preparation, feature engineering, model selection, training, and evaluation based on historical trends. Utilizing supervised learning methodologies, these models evaluate critical variables such transaction amount, geographical alterations, time of day, and merchant risk to ascertain the likelihood of fraud.

Diverse machine learning techniques, such as Logistic Regression, Decision Trees, Random Forests, XGBoost, and Neural Networks, provide varying degrees of accuracy and interpretability. Although traditional models such as Logistic Regression are efficient and rapid, sophisticated methods like Neural Networks and Gradient Boosting yield superior accuracy by identifying intricate fraud patterns. Post-training, the model undergoes evaluation utilizing critical performance metrics like accuracy, precision, recall, and F1-score to ascertain its efficacy in detecting fraudulent transactions while reducing false positives.

Upon deployment, the fraud detection system functions in real time, scrutinizing each transaction and identifying questionable ones for additional examination. This proactive strategy assists financial organizations in reducing fraud losses and bolstering client trust. Fraud trends are constantly evolving, necessitating regular model updates, retraining, and adaptive thresholding to ensure accuracy. Moreover, the integration of AI with rule-based systems and human fraud analyzers enhances fraud detection initiatives.

References

1. Axelsson, S. (2000). Intrusion detection systems: A survey and taxonomy. In Proceedings of the 6th ACM Conference on Computer (pp. [page numbers needed]). ACM.
2. Bello, O. (2024). Challenges in AI-driven fraud detection: Dataset quality and regulatory compliance issues. International Journal of Cybersecurity and Digital Forensics, 5(1), 25–40.
3. Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. Decision Support Systems, 50(3), 602–613.
4. Blunt, G., & Hand, D. J. (2000). The UK credit card market (Technical Report). Department of Mathematics, Imperial College.
5. Bolton, R. J., & Hand, D. J. (2001). Unsupervised profiling methods for fraud detection. In Proceedings of the Conference on Credit Scoring and Credit Control.
6. Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. Statistical Science, 17(3), 235–255.
7. Coralogix. (2025, March 13). A Guide to ML Fraud Detection monitoring & model performance. https://coralogix.com/ai-blog/how-to-optimize-ml-fraud-detection-a-guide-to-monitoring-performance/
8. Corderre, D. (1999). Fraud detection: Using data analysis techniques to detect fraud. Global Audit Publications.
9. Dar, B. I. (2024). AI and machine learning in financial fraud prevention: A security approach. Journal of Financial Security, 12(3), 89–102.
10. Dubey, S. (2022). Role of AI in fraud detection for Indian banks: Challenges and opportunities. Indian Banking Review, 9(2), 45–60.
11. Duman, E., & Ozcelik, M. H. (2011). Detecting credit card fraud by genetic algorithm and scatter search. Expert Systems with Applications, 38(10), 13057–13063.
12. Eludire, B. (2023). Economic implications of AI in revolutionizing fraud detection within financial markets. Journal of Financial Economics, 22(1), 15–30.
13. Farman, A. (2023). Applicability of machine learning in fraud detection across various industries. International Journal of Business Analytics, 9(4), 100–115.
14. Francisca, N. O. (2011). Data mining application in credit card fraud detection system. Journal of Engineering Science and Technology, 6(3), 311–322.
15. GeeksforGeeks. (2025, February 27). Understanding the confusion matrix in machine learning. GeeksforGeeks. https://www.geeksforgeeks.org/confusion-matrix-machine-learning/
16. Ghosh, S., & Reilly, D. L. (1994). Credit card fraud detection with a neural-network. In Proceedings of the Annual International Conference on System Science (pp. 621–630).
17. Hand, D. J. (2007). Mining personal banking data to detect fraud. In Selected contributions in data analysis and classification (pp. 377–386). Springer.
18. Holmes, G., Donkin, A., & Witten, I. H. (1994). Weka: A machine learning workbench. In Proceedings of the 2nd Australia and New Zealand Conference on Intelligent Information Systems.
19. Ismaeil, M. K. A. (2024). Enhancing financial security through AI-driven fraud detection systems. Global Financial Review, 18(4), 101–118.
20. Kaggle: your machine learning and data science community. (n.d.). https://www.kaggle.com/
21. Kamuangu, P. (2024). Future challenges and innovations in AI-based fraud detection. Financial Intelligence Journal, 11(2), 55–72.
22. Kou, Y., Lu, C.T., Sirwongwattana, S., & Huang, Y.P.(2004). Survey of fraud detection techniques. In Proceedings of the IEEE International Conference on Networking, Sensing and Control (Vol. 2).
23. Maes, S., Tuyls, K., Vanschoenwinkel, B., & Manderick, B.(1993). Credit card fraud detection using Bayesian and neural networks.In Proceedings of the 1st International NAISO Congress on Neuro Fuzzy Technologies (pp.261-270).

24. Machine Learning. (2024, October 3). Accuracy, precision, recall, and F1-Score. Machine Learning Tutorials, Courses and Certifications. https://machinelearning.org.in/accuracy-precision-recall-and-f1-score/
25. Mohammed,A.(2024). The future of AI adoption in the private sector for enhanced fraud detection capabilities in Saudi Arabia.Saudi Journal of Business Administration,8(2),70-85.
26. Mohanty,B.(2023).AI solutions in fraud detection: Enhancing security and efficiency.Journal of Business Technology,14(1),23-41.
27. Mujtaba,H.(2024).Predictive analytics in AI-driven fraud prevention: Real-time risk assessment strategies.Journal of Risk Management,10(1),45-60.
28. Ngai,E.W.T.,Hu,Y.,Wong,Y.H.,Chen,H.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.
29. Nwankwo,E.(2024).The impact of AI on fraud detection in financial services.AI & Finance Journal,17(3),67-85.
30. Pan,Y.(2024).Utilizing CNNs and RNNs for processing transactional data in fraud detection.International Journal of Machine Learning and Cybernetics,15(5),150-165.
31. Phua,C.,Lee,V.,Smith,K.,&Gayler,R.(2005).A comprehensive survey of data mining-based fraud detection research.Artificial Intelligence Review.
32. Qatawneh,M.(2024).Enhancing AI-driven fraud detection with natural language processing techniques.Journal of Financial Crime,31(2),120-135.
33. Quah,J.T.S.&Sriganesh,M.(2008).Real-time credit card fraud detection using computational intelligence.Expert Systems with Applications,35(4),1721-1732.
34. Sharma,C.(2023).Fraud detection in financial institutions: The role of AI and ML.Journal of Computational Finance,10(2),29-47.
35. Sharma,R.(2023).Effectiveness of machine learning models in distinguishing fraudulent transactions.Journal of Financial Services Research,15(1),78-92.
36. Srivastava,A.,Kundu,A.,Sural,S.,&Mazumdar,A.K.(2008).Credit card fraud detection using hidden Markov model.IEEE Transactions on Dependable and Secure Computing,5(1),37-48.
37. Tiwari,P.(2023).Bibliometric analysis of AI-driven fraud detection post-pandemic.Journal of Business Research,18(2),200-215.
38. Tiwari,R.(2023).AI-driven fraud detection: Addressing ethical and regulatory challenges.Regulatory Compliance Review,8(4),112-130.
39. Witten,I.H.,Frank,E.,&Hall,M.A.(2011).Data mining: Practical machine learning tools and techniques (3rd ed.). Morgan Kaufmann.
40. Xu,J.(2024).Deep learning for fraud detection: Anomaly detection in financial transactions.Neural Networks in Finance,19(2),79-98.
41. Zareapoor,M.,Seeja,K.R.,&Alam,A.M.(2012).Analyzing credit card fraud detection techniques based on certain design criteria.International Journal of Computer Application,52(3),35-42.
42. Zaslavsky,V.&Strizhak,A.(2006).Credit card fraud detection using self-organizing maps.Information & Security,18,48-63.

HOW TO CITE THIS ARTICLE: Ahuja, E. K., & Komal. (2025). Role of AI in financial fraud detection. *Sudarshan Research Journal*, *3*(3), 1–7.