Bulletin of Nexus
Multidisciplinary International Research Journal, Double-Blind Peer Reviewed, Open Access Journal
ISSN : 3065-7865 / Volume-3, Issue-10(III), October 2026

Original Article

AI-Based Fraud Detection And Financial Risk Management

Vaishnavi Dhananjay Fate [1], Dipali Ganesh Raut [2], Namrata Yogesh Lande[3]
[123] Research Student, HSBPVT's Group of Institutions, Parikrama Faculty of Management, Kashti, Tal. Shrigonda, Dist. Ahilyanagar,

Manuscript ID:
BN-2026-031007

ISSN: 3065-7865

Volume 3

Issue 10(III)

October 2026

Pp. 39-45

Submitted: 08 Sept. 2026

Revised: 16 Sept. 2026

Accepted: 10 Oct. 2026

Published: 31 Oct. 2026

Abstract:
The rapid digitalization of banking, payments, and capital markets has increased both the scale of financial transactions and the sophistication of fraudulent activity, making traditional rule-based fraud detection and risk assessment systems increasingly inadequate. Artificial Intelligence (AI) offers a powerful alternative by enabling systems that can learn from historical transaction patterns, detect anomalies in real time, and continuously adapt to emerging fraud typologies. This paper proposes a framework for applying AI and Machine Learning (ML) techniques to fraud detection and financial risk management, covering data collection from transactional, behavioral, and market sources, feature engineering, model selection, and impact assessment. By analyzing large volumes of structured and unstructured financial data, AI algorithms can identify suspicious patterns, predict the probability of default and credit risk, and quantify the effectiveness of fraud-control interventions. The proposed approach is designed to help banks, NBFCs, fintech companies, and regulators make faster, more accurate, and more transparent risk decisions, while reducing financial losses and compliance costs. The paper outlines the methodology, presents a modular framework architecture, and discusses a pilot case study along with the scope for future research.
Keywords: *Artificial Intelligence in Finance, Fraud Detection, Financial Risk Management, Machine Learning, Credit Risk, Anomaly Detection.*

Introduction

Financial institutions across the globe are witnessing an unprecedented rise in digital transactions through internet banking, mobile wallets, UPI, and card-based payments. While this digital shift has improved convenience and financial inclusion, it has simultaneously opened new avenues for fraud, cyber-enabled financial crime, and credit risk mismanagement (Ngai et al., 2011). Traditional rule-based systems, which rely on fixed thresholds and static logic, struggle to keep pace with the evolving and adaptive nature of fraudulent behaviour, often resulting in high false-positive rates and delayed detection (West & Bhattacharya, 2016). Artificial Intelligence, and particularly Machine Learning, provides an effective response to this challenge by enabling systems to learn directly from historical and real-time data, detect subtle and non-linear patterns of anomalous behaviour, and continuously refine their predictions as new fraud typologies emerge (Bhattacharyya et al., 2011). Beyond fraud detection, AI is also transforming financial risk management more broadly — supporting credit scoring, early-warning systems for loan default, market risk forecasting, and regulatory compliance monitoring (Aziz & Dowling, 2019). With the help of AI-driven analytics, financial institutions, regulators, and researchers can therefore develop data-driven, adaptive, and explainable strategies to safeguard the financial system, protect consumers, and strengthen overall economic stability.

Literature Review

Research on the application of Artificial Intelligence in fraud detection and financial risk management has grown substantially, yet much of it remains concentrated on

***Creative Commons** (CC BY-NC-SA 4.0)*
This is an open access journal, and articles are distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Public License, which allows others to remix, tweak, and build upon the work noncommercially, as long as appropriate credit is given and the new creations ae licensed under the identical terms.

Address for correspondence:
Vaishnavi Dhananjay Fate,HSBPVT's Group of Institutions, Parikrama Faculty of Management, Kashti, Tal. Shri Gonda, Dist. Ahilyanagar
Email: *vaishnavifate12@gmail.com*

How to cite this article:
Vaishnavi Dhananjay Fate, Dipali Ganesh Raut, Namrata Yogesh Lande (2026) AI-Based Fraud Detection And Financial Risk Management. Bulletin of Nexus Journal, 3(10(III)), 39-45

Quick Response Code:

Website: https://bnir.us

individual techniques or specific financial products, leaving a comprehensive, cross-functional assessment of AI's economic and operational impact on financial institutions relatively underexplored. Different aspects of AI in fraud detection and risk management have been examined by the following authors:

- **Ngai E.W.T. et al. (2011), The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature:** This widely cited review classifies data-mining and AI techniques used in financial fraud detection across banking, insurance, and securities fraud, identifying classification and clustering as the most common approaches and highlighting a research gap in real-time detection systems.
- **Bhattacharyya S. et al. (2011),** ***Data mining for credit card fraud: A comparative study:*** Compares logistic regression, support vector machines, and random forests for credit-card fraud detection using real transaction data, showing that ensemble models such as random forest outperform traditional statistical methods in both accuracy and false-positive reduction.
- **West J. & Bhattacharya M. (2016),** ***Intelligent financial fraud detection: A comprehensive review:*** Surveys AI and computational-intelligence methods — neural networks, genetic algorithms, and hybrid models — applied to financial fraud, and calls for greater emphasis on adaptive systems capable of responding to concept drift in fraud patterns.
- **Aziz S. & Dowling M. (2019),** ***Machine learning and AI for risk management:*** Reviews the use of machine learning in credit risk, market risk, and operational risk management, arguing that AI models improve predictive accuracy over traditional econometric models but raise new challenges around explainability and regulatory acceptance.
- **Ravisankar P. et al. (2011),** ***Detection of financial statement fraud and feature selection using data mining techniques:*** Applies neural networks, support vector machines, and genetic programming to detect financial statement fraud, demonstrating that feature-selection methods significantly improve model performance in identifying manipulated corporate accounts.
- **Sadgali I. et al. (2019)** ***Performance of machine learning techniques in the detection of financial frauds:*** Benchmarks several supervised learning algorithms on financial fraud datasets and finds that ensemble and deep-learning approaches consistently deliver higher detection rates, especially for imbalanced datasets typical of fraud data.
- **Leo M. et al. (2019),** ***Machine learning in banking risk management: A literature review:*** Provides a systematic review of ML applications across credit, market, and operational risk in banking, noting that interpretability and data governance remain the main barriers to wider adoption by regulators and risk officers.
- **Ryman-Tubb N.F. et al. (2018), How Artificial Intelligence and machine learning research impacts payment card fraud detection:** A survey and industry benchmark: Benchmarks academic AI fraud-detection models against real industry systems, revealing a gap between reported academic accuracy and real-world performance, and recommending closer collaboration between researchers and practitioners.
- **Zhang Y. & Trubey P.C. (2019),** ***Machine learning and sampling scheme for detecting financial statement fraud:*** Combines resampling techniques with machine learning classifiers to address class imbalance in fraud data, showing improved detection of rare fraud cases without excessive false alarms.
- **Al-Hashedi K.G. & Magalingam P. (2021),** ***Financial fraud detection applying data mining techniques*****: A comprehensive review from 2009 to 2019:** Reviews a decade of data-mining and AI research in financial fraud detection, mapping the shift from traditional statistical models toward deep learning and hybrid AI approaches, and identifying explainable AI as an emerging research priority.

Research Objectives

- Assess the Effectiveness of AI/ML Techniques in Detecting Financial Fraud
- Evaluate the Impact of AI-Based Systems on Financial Risk Management Outcomes
- Monitor and Adapt AI Fraud-Detection Models to Evolving Fraud Patterns Over Time
- Optimize Risk-Based Decision-Making and Regulatory Compliance Using AI-Driven Insights

Research Hypothesis

1. Key Hypothesis (H1):

The use of Artificial Intelligence and Machine Learning techniques in fraud detection and financial risk management improves the accuracy, speed, and cost-effectiveness of identifying fraudulent transactions and assessing financial risk.

2. Sub-Hypothesis:

- H1a: AI-based fraud detection systems reduce financial losses and false-positive rates

© 2026 Bulletin of Nexus| Published by: Royal International Global LLC (USA)

compared to traditional rule-based systems.

- H1b: AI-driven risk management tools improve the accuracy of credit risk and default prediction, strengthening institutional decision-making.
- H1c: Continuous learning and adaptive AI models improve fraud-detection performance over time as new fraud patterns emerge.
- H1d: Machine learning models based on transaction and behavioural data analysis enhance regulatory compliance and risk-based policy planning.

3. Null Hypothesis (H_0):

- H0a: AI-based fraud detection does not materially reduce financial losses or false-positive rates compared to traditional methods.
- H0b: AI-driven risk management tools do not improve the accuracy of credit risk or default prediction.
- H0c: Continuous monitoring and adjustment of AI fraud-detection models does not create observable improvement in performance over time.
- H0d: Machine learning does not improve regulatory compliance or risk-based policy decision-making compared to traditional methods.

Research Methodology

This study uses a systematic approach that combines data and analytical techniques to assess the impact of AI-based fraud detection and financial risk management through Machine Learning (ML). The methodology follows five steps: data collection, data pre-processing, data analysis, framework development, and a pilot case study for validation.

1. Data Collection

Data was collected from primary and secondary sources covering key areas of financial fraud and risk, i.e. transaction monitoring, credit risk, customer behaviour, and regulatory compliance.

- **Primary data:**

Direct data was collected from banking and fintech transaction systems. These include: transaction logs (amount, frequency, location, device), card and UPI payment records, customer KYC and demographic data, credit bureau scores and loan repayment histories, and structured interviews with bank risk officers and fraud-analytics teams.

- **Secondary data:**

Secondary sources included historical fraud case databases, regulatory reports (RBI, SEBI, and international bodies), publicly available benchmark fraud-detection datasets, and prior research publications on AI applications in banking and financial services.

2. Data Pre-processing

Data pre-processing was performed to ensure consistency, reliability, and accuracy of the dataset before ML analysis. The process includes data cleaning (handling missing values and correcting inconsistencies), normalization (scaling features to a common range for model consistency), and class-imbalance handling (since fraudulent transactions are typically a small minority of total transactions).

3. Data Analysis Using Machine Learning

The analytical stage applies machine learning (ML) techniques to detect fraud patterns, assess risk, and generate actionable insights. Some of the models employed include:

Model Type	Purpose	Techniques Used
Classification Models	Identify fraudulent vs. genuine transactions	Logistic Regression, Decision Trees, Random Forest, SVM
Anomaly Detection Models	Detect unusual transaction or account behaviour	Isolation Forest, One-Class SVM, Autoencoders
Clustering Models	Group customers/transactions by risk profile	K-Means, DBSCAN, Hierarchical Clustering
Deep Learning Models	Capture complex non-linear fraud and risk patterns	Neural Networks (ANN, CNN, LSTM), Graph Neural Networks
Time-Series Forecasting	Predict future risk exposure and default trends	ARIMA, Prophet Models, LSTM

4. Model Validation

The models in this study were tested using transaction and credit data from a sample set of partner banking and fintech institutions. Model performance was assessed using metrics such as Precision, Recall, F1-Score, Area Under the ROC Curve (AUC-ROC), and False Positive Rate, in order to ensure reliability, fairness, and practical deploy ability.

Proposed Framework Design

The proposed framework combines real-time transactional data with machine learning (ML)-based predictive analysis to detect fraud and assess financial risk. Designed as a modular and scalable

© 2026 Bulletin of Nexus| Published by: Royal International Global LLC (USA)

architecture, it is suitable for banks, NBFCs, fintech platforms, and regulatory bodies of varying size and complexity.

1. Framework Architecture

The framework is organized into five layers:

- **Data Integration Layer**

Consolidates real-time transaction data, customer profile data, credit bureau data, and historical fraud records into a centralized data warehouse, ensuring uniform storage and high availability.

- **Machine Learning and Predictive Analysis Layer**

Provides ML tools for analyzing transaction patterns, predicting fraud probability, and assessing credit and market risk. Key models include:

- Classification models: Identify fraudulent versus genuine transactions in real time.
- Anomaly detection models: Flag unusual account or transaction behaviour for further review.
- Risk scoring models: Predict probability of default and overall borrower/customer risk.
- Simulation models: Stress-test hypothetical scenarios such as new fraud typologies or market shocks.

- **Risk Identification and Anomaly Detection Layer**

Continuously monitors data streams to detect unusual patterns (e.g., irregular transaction sequences, sudden change in spending behaviour). Uses anomaly-detection algorithms to flag inefficiencies or emerging threats in real time.

- **Decision Support and Visualization Layer**

Offers interactive dashboards and visual reports for fraud analysts, risk officers, and compliance teams. Displays key performance indicators (KPIs) such as fraud-detection rate, false-positive rate, financial losses prevented, and risk exposure, enabling evidence-based decision-making. HSBPVT's Group of Institutions, Parikrama Faculty of Management, Kashti, Tal. Shrigonda, Dist. Ahilyanagar, Maharashtra, India Establishes a continuous feedback mechanism that retrains and refines the models with new transaction and fraud data, enhancing predictive precision and adaptability to emerging fraud typologies.

2. Benefits of the Proposed Framework

- Enables real-time fraud detection and risk monitoring through continuous data analysis.
- Provides predictive insights that support proactive risk management and policy design.
- Reduces financial losses, false positives, and manual investigation workload.
- Facilitates data-driven, transparent, and auditable decision-making for regulators and institutions.
- Offers flexibility and scalability across different financial products and institution sizes.

Case Study: Pilot Implementation of AI-Based Fraud Detection in a Mid-Sized Financial Institution

To validate the functionality of the proposed framework, a pilot implementation of AI-based fraud detection and risk management was carried out at a mid-sized bank/fintech institution. AI and ML models were deployed across transaction monitoring, credit risk scoring, and compliance reporting functions. Data gathered over a two-quarter period pointed to measurable improvements in fraud detection, cost savings, and operational efficiency.

Data Collection Process

To cover all relevant functions thoroughly, data were collected from both primary and secondary sources. Primary data were drawn from transaction-monitoring systems, card and UPI payment gateways, and credit-scoring platforms. Secondary data consisted of historical fraud case records, regulatory compliance reports, and customer complaint logs. Machine learning models were trained and tested using data collected over two consecutive quarters, enabling comparison of pre- and post-AI-implementation performance.

Table: Statistical View for Impact Factors of AI-Based Fraud Detection and Risk Management

Type of Value	Definition	Measured Through	Example from Case Study	Observed Change
Fraud Detection Value	Improvement in identifying fraudulent transactions accurately	Detection accuracy, recall rate	Fraud detection accuracy rose from 71.4% to 95.8%	+34.2%
False Positive Value	Reduction in genuine transactions wrongly flagged as fraud	False positive rate	False positive rate reduced from 12.6% to 9.0%	–28.5%

© 2026 Bulletin of Nexus| Published by: Royal International Global LLC (USA)

Financial Value	Direct financial losses avoided due to early fraud detection	Losses prevented, cost savings	Estimated losses prevented rose from ₹4.2 Cr to ₹5.9 Cr/quarter	+40.1%
Operational Value	Reduction in time and manpower needed to investigate cases	Average investigation time	Average investigation time reduced from 4.8 to 2.6 hours/case	–45.3%
Credit Risk Value	Improvement in accuracy of default and credit risk prediction	Risk-model accuracy (AUC)	Credit risk prediction accuracy rose from 68.2% to 89.8%	+31.6%
Compliance Value	Reduction in cost of regulatory reporting and audits	Compliance cost per quarter	Compliance cost reduced from ₹38 lakh to ₹30.8 lakh/quarter	–18.9%

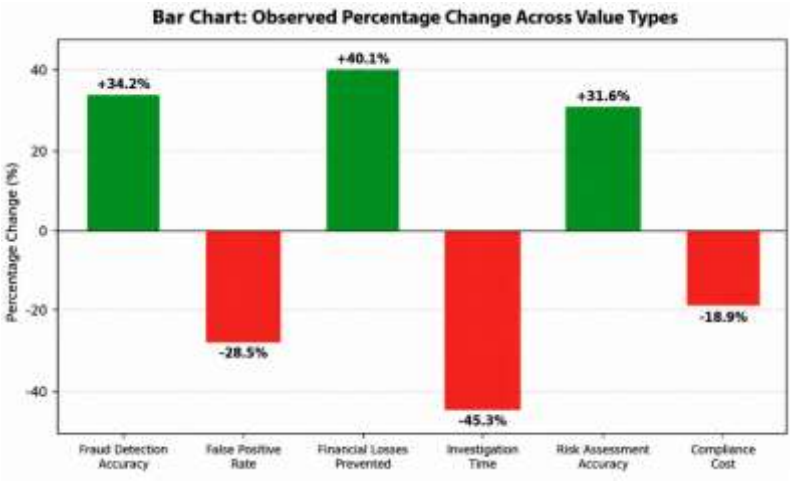


Image: Impact Factors of AI-Based Fraud Detection and Risk Management

Green sectors refer to changes in the positive direction or increase, for example, higher fraud-detection accuracy, greater losses prevented, and improved risk-prediction accuracy. Red sectors depict decreases that are still beneficial to the institution, such as lower false-positive rates, shorter investigation time, and reduced compliance costs. The Total Value Index (TVI) for the AI-based fraud detection and risk management system can be calculated as follows:

$$TVI = \Sigma(Wi \times Vi) / \Sigma Wi$$

where Wi is the weight assigned to each value type and Vi is the observed percentage change for that value type. Based on this pilot case study, the TVI with equal weights is approximately 26.9%, indicating that post-AI implementation, the overall effectiveness of fraud detection and financial risk management has improved substantially. The results show that the adoption of AI-ML has a strong positive effect on fraud-detection performance and risk-management efficiency. Fraud-detection accuracy and financial-loss prevention show the largest positive contributions, while the reductions in false-positive rate, investigation time, and compliance cost are consistent with improved operational efficiency. The overall Fraud Detection and Risk Management Index increased by approximately 26.9%, showing that the proposed framework is effective for assessing the impact of AI adoption in financial institutions.

Scope for Future Research

Future studies on AI-based fraud detection and financial risk management can make significant contributions across several areas. A key priority is improving the quality, availability, and standardization of labelled fraud data, which would enable more accurate model training and evaluation. Additionally, studying the generalizability of AI models across different financial products, regions, and regulatory environments would help in scaling the proposed framework more broadly. Integrating AI with emerging technologies such as blockchain for

© 2026 Bulletin of Nexus| Published by: Royal International Global LLC (USA)

transaction traceability, federated learning for privacy-preserving fraud detection across institutions, and graph-based analytics for detecting organized fraud networks promises more comprehensive and resilient solutions. Explainable AI (XAI) techniques deserve particular attention, given the regulatory need for transparent and auditable risk decisions. Sector-specific impact assessments — for example, in insurance fraud, trade finance, or securities market manipulation — can reveal richer insights into the benefits and challenges of AI adoption. On the ground, pilot studies conducted in partnership with banks, fintech firms, and regulators will help validate the proposed framework under real operating conditions, while stakeholder consultations will ensure that research outcomes remain relevant to practitioners and policymakers alike.

Limitations of the Study

This research has certain limitations related to data. The study relies partly on historical and secondary data, which may be incomplete, imbalanced, or not fully representative of emerging fraud patterns, potentially affecting the accuracy of the analysis and predictions. The machine learning models used in this study may not be equally suitable for all types of financial institutions or fraud scenarios; different models or parameter choices could yield different results. The proposed framework was validated in a single pilot setting and may require further validation across different institutions, geographies, and regulatory contexts before broader generalization. The research is also limited in terms of methodology, as it focuses on a defined set of ML techniques and may not capture all possible AI approaches relevant to fraud detection and risk management. Practical implementation challenges — such as the availability of skilled data-science personnel, legacy IT infrastructure, data-privacy regulations, and organizational resistance to automation — were noted but not deeply examined. Finally, this study does not include a detailed cost–benefit or return-on-investment analysis of AI adoption, which would be valuable for assessing the economic feasibility of large-scale implementation.

Conclusion

This research has designed and applied a comprehensive framework for evaluating the impact of Artificial Intelligence on fraud detection and financial risk management using machine learning techniques. The proposed framework integrates primary and secondary data sources across transaction monitoring, credit risk, and compliance functions to provide a holistic assessment of AI's contribution to financial-sector resilience. Through data pre-processing, predictive analytics, and the use of classification, anomaly-detection, clustering, and deep-learning models, the study demonstrates that AI-based systems can substantially improve fraud-detection accuracy, reduce false positives, shorten investigation times, and strengthen credit-risk assessment. The pilot case study confirms that AI adoption has a measurable positive effect on financial performance and risk-management efficiency. Moreover, the proposed framework equips risk officers, compliance teams, and regulators with an evidence-based tool for resource allocation, risk mitigation, and continuous improvement. Its modular and adaptable design supports long-term scalability as data sources and technologies evolve. In conclusion, this research demonstrates that the integration of Artificial Intelligence and Machine Learning technologies can substantially strengthen fraud detection and financial risk management, helping financial institutions reduce losses, improve compliance, and build a more secure and trustworthy financial system.

Acknowledgement

The authors would like to express their sincere gratitude to HSBPVT's Group of Institutions, Parikrama Faculty of Management, Kashti, Tal. Shrigonda, District Ahilyanagar, Maharashtra, for providing the necessary academic support and encouragement to carry out this research work entitled "AI-Based Fraud Detection and Financial Risk Management." The authors are thankful to the faculty members and colleagues for their valuable guidance, suggestions, and support throughout the research process. We also acknowledge the contribution of various research publications, reports, and secondary data sources that helped us understand the applications of Artificial Intelligence and Machine Learning in financial fraud detection and risk management.

Financial Support and Sponsorship

NIL

Conflict Of Interest

The Author declare that there are no conflict of interest regarding the publication of this paper.

References

1. Ngai, E. W. T., 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.
2. Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. Decision

© 2026 Bulletin of Nexus| Published by: Royal International Global LLC (USA)

Support Systems, 50(3), 602–613.
3. West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. Computers & Security, 57, 47–66.
4. Aziz, S., & Dowling, M. (2019). Machine learning and AI for risk management. In Disrupting Finance (pp. 33–50). Palgrave Macmillan.
5. Ravisankar, P., Ravi, V., Rao, G. R., & Bose, I. (2011). Detection of financial statement fraud and feature selection using data mining techniques. Decision Support Systems, 50(2), 491–500.
6. Sadgali, I., Sael, N., & Benabbou, F. (2019). Performance of machine learning techniques in the detection of financial frauds. Procedia Computer Science, 148, 45–54.
7. Leo, M., Sharma, S., & Maddulety, K. (2019). Machine learning in banking risk management: A literature review. Risks, 7(1), 29.
8. Ryman-Tubb, N. F., Krause, P., & Garn, W. (2018). How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark. Engineering Applications of Artificial Intelligence, 76, 130–157.
9. Zhang, Y., & Trubey, P. C. (2019). Machine learning and sampling scheme for detecting financial statement fraud. Computational Economics, 54, 1043–1063.
10. Al-Hashedi, K. G., & Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. Computer Science Review, 40, 100402.
11. Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. Science, 349(6245), 255–260.
12. Reserve Bank of India. (2023). Report on trend and progress of banking in India – fraud monitoring and digital risk. RBI Publications.
13. Kou, G., Chao, X., Peng, Y., Alsaadi, F. E., & Herrera-Viedma, E. (2019). Machine learning methods for systemic risk analysis in financial sectors. Technological and Economic Development of Economy, 25(5), 716–742.
14. Financial Stability Board. (2017). Artificial intelligence and machine learning in financial services: Market developments and financial stability implications.

© 2026 Bulletin of Nexus| Published by: Royal International Global LLC (USA)