Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 10, NCREHAASTE - 2026

Impact of AI on Financial Fraud Detection and Risk Management in Modern Businesses

Upasna Sharma
MBA II Year
Department of Management
MIT Moradabad
sharmaupasna84@gmail.com

Neha Chauhan
MBA II Year
Department of Management
MIT Moradabad
n42505431@gmail.com

Abdul Ahad
BBA III Year
Department of Management
MIT Moradabad
abdulahaddr1@gmail.com

Shweta Gupta
Assistant Professor
Department of Management
MIT Moradabad
gggupta.shweta7@gmail.com

***Abstract*—Artificial Intelligence (AI) has emerged as an important technology for modern businesses, particularly in finance, banking, accounting, payments and risk management. The rapid growth of digital banking, online payments, e-commerce and technology-based transactions has created enormous volumes of financial data. While digitalisation improves speed, convenience and efficiency, it also creates new opportunities for financial fraud. Traditional fraud detection methods that depend mainly on predefined rules and manual checking may not identify sophisticated and continuously changing fraudulent behaviour. This research paper examines the impact of AI on financial fraud detection and risk management in modern businesses. It focuses on the use of Machine Learning, Deep Learning, anomaly detection, predictive analytics and automated monitoring. The study uses secondary data from academic literature, institutional reports and reliable published sources. The research follows a descriptive and analytical design. The analysis indicates that AI can improve the speed, scalability and efficiency of fraud detection and can support proactive risk management. AI can identify unusual transaction patterns, generate alerts and support risk-based decisions. At the same time, data quality, privacy, cybersecurity, explainability, algorithmic bias, implementation cost and human oversight remain important concerns. The study concludes that AI can strengthen financial security when it is implemented responsibly and combined with effective governance and human judgement.**

***Keywords*—Artificial Intelligence, Financial Fraud, Fraud Detection, Risk Management, Machine Learning, Deep Learning, Financial Technology, Modern Businesses.**

I. INTRODUCTION

Technology has changed the structure of modern business. Financial transactions that were once conducted mainly through physical branches and paper-based processes are increasingly completed through digital platforms. Customers can transfer money, make purchases, apply for loans, pay bills and access financial services through mobile phones and computers. Businesses also use digital accounting, enterprise systems, online payment gateways and data analytics.

This digital transformation has created substantial benefits. Organisations can process transactions faster, serve customers across geographical boundaries and use data to improve business decisions. However, the same digital environment can be exploited by individuals and organised groups for fraudulent purposes. Fraudsters can use stolen credentials, manipulated information, fake accounts, unusual transaction patterns and other techniques to obtain financial benefits.

Financial fraud can cause direct monetary losses, but its impact is broader. A serious fraud incident may damage an organisation's reputation,

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 10, NCREHAASTE - 2026

reduce customer trust, increase investigation costs, create regulatory problems and affect long-term business performance. Therefore, fraud prevention is an important component of financial risk management.

Traditional fraud detection often uses predefined rules. For example, a system may flag a transaction when the amount exceeds a threshold or when the transaction takes place in an unusual location. Such rules remain useful, but they may struggle when fraudsters change their behaviour. Modern businesses therefore require methods that can learn from data and identify complex patterns.

Artificial Intelligence offers such capabilities. AI systems can process large quantities of information, recognise patterns, detect anomalies and support predictions. Machine Learning can learn from historical transactions, while Deep Learning can identify complex relationships within large datasets. AI can therefore support a transition from reactive fraud investigation to proactive monitoring.

This paper studies the role of AI in financial fraud detection and risk management and discusses its benefits, challenges, ethical issues and future scope.

II. BACKGROUND OF ARTIFICIAL INTELLIGENCE IN FINANCIAL MANAGEMENT

Artificial Intelligence refers broadly to computer-based systems capable of performing tasks associated with human intelligence, such as learning, classification, prediction, pattern recognition and decision support. In financial management, AI is increasingly connected with large-scale data analysis and automated monitoring.

Machine Learning is particularly important because it enables a system to learn patterns from historical data. In supervised learning, examples are labelled as fraudulent or legitimate and the model learns to distinguish between them. In unsupervised learning, the system searches for unusual structures or patterns without requiring every transaction to be labelled.

Deep Learning uses multi-layer neural networks to identify complex relationships. It can be useful when the financial dataset is large and contains multiple variables. Natural Language Processing can also assist finance teams by analysing textual information such as reports, customer communications and other documents.

Predictive analytics is another important application. Instead of simply describing what has happened, predictive systems attempt to estimate what may happen in the future. In risk management, this can support early-warning systems and help managers prioritise potential risks.

The increasing availability of computing power, cloud platforms and digital data has made AI more accessible to businesses. However, successful adoption depends on data quality, technical capability, governance and skilled employees. AI should therefore be considered not simply as an automation tool but as part of a broader financial management framework.

III. FINANCIAL FRAUD IN MODERN BUSINESSES

A. Transaction Fraud

Transaction fraud involves unauthorised or deceptive financial transactions. It can occur through payment systems, bank transfers, digital wallets or online platforms. AI can compare current activity with normal transaction behaviour and flag unusual activity.

B. Credit Card Fraud

Credit card fraud involves unauthorised use of card information. Online commerce increases the number of transactions that must be monitored. AI can consider transaction amount, timing, location, merchant information and behavioural patterns.

C. Accounting Fraud

Accounting fraud involves intentional manipulation or misrepresentation of financial

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 10, NCREHAASTE - 2026

information. AI-based analytics can help identify unusual relationships between accounting variables and highlight records that require human review.

D. Identity Fraud

Identity fraud occurs when personal information is misused for financial gain. AI-supported identity verification and behavioural analysis can assist organisations in identifying suspicious account activity.

E. Payment Fraud

Payment fraud may involve fake payment instructions, unauthorised transfers or manipulated payment information. Automated monitoring can help organisations respond more quickly.

F. Internal Fraud

Internal fraud is committed by employees or individuals with access to organisational systems. Behavioural analytics can identify unusual access patterns, transactions or activity. The variety of fraud types demonstrates why organisations need flexible detection systems. A fraud-management programme must combine technology, internal controls, employee awareness and investigation procedures.

TABLE I
TYPOLOGY OF FINANCIAL FRAUD AND AI DETECTION MECHANISMS

Fraud Category	Primary Vectors	Limitations of Traditional Controls	AI/ML Detection Mechanism
Real-Time Payments	QR manipulation, collect-request phishing, remote access apps.	Post-transaction alerts allow funds to be transferred before review.	Sub-second predictive scoring of payee data, device telemetry, and behaviour.
Credit/Debit Cards	Credential harvesting, card-not-present online gateways.	Static thresholds lead to elevated false rejections for genuine cardholders.	Contextual velocity models, merchant profiling, and geolocation checks.
Identity & KYC Fraud	Manipulated documents, synthetic IDs, deepfake verification.	Manual checks miss pixel tampering and digital manipulation.	Deep learning facial liveness verification and automated registry checks.
Mule Account Rings	Layered transfers across low-tier and dormant accounts.	Isolated bank audits fail to trace cross-institutional fund hops.	Graph Neural Networks mapping interconnected transaction networks.
Accounting Fraud	Circular trading, invoice inflation, fund diversion.	Periodic retrospective audits identify discrepancies months later.	Predictive NLP models reconciling statements, ledgers, and tax returns.
Internal Fraud	System overrides, unauthorised limit increases, data extraction.	Static role permissions lack behavioral visibility.	User and Entity Behaviour Analytics (UEBA) flagging anomalous employee actions.

IV. LITERATURE REVIEW

Research on AI in finance has expanded rapidly. Ahmed, Alshater, Ammari and Hammami (2022) [1] reviewed research on Artificial Intelligence and Machine Learning in finance and showed the broad growth of AI applications across financial activities. Their work indicates that AI is becoming an important component of modern financial research.

Studies of AI-based fraud detection generally identify machine learning as a promising approach because it can analyse large numbers of

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 10, NCREHAASTE - 2026

transactions and learn patterns associated with suspicious behaviour. Compared with purely rule-based approaches, machine learning can potentially adapt to more complex patterns.

Research into deep learning has also examined financial fraud detection. Deep learning models can process large and complex datasets and may capture relationships that are difficult to represent through simple rules. However, these methods may require substantial data and computing resources.

Research on AI-based credit scoring and risk management has highlighted the potential for AI to analyse multiple variables and support financial risk assessment [9]. At the same time, concerns have been raised regarding fairness, transparency, explainability and responsible implementation.

Giudici, Centurelli and Turchetta (2024) [3] emphasised that AI risk measurement should consider more than predictive accuracy. Risk, fairness and explainability are also important when AI is used in financial decision-making.

The Bank for International Settlements (2024) [2] has discussed governance, data, cybersecurity, model risk and regulatory issues associated with AI in finance. These issues demonstrate that technological performance must be accompanied by appropriate controls.

Recent literature also identifies class imbalance, privacy, explainability and changing fraud patterns as continuing challenges [6], [10]. Fraudulent transactions are usually much less common than legitimate transactions, which makes model development difficult.

Overall, the literature supports the potential of AI while emphasising that technology cannot completely eliminate fraud. Effective implementation requires reliable data, human supervision, governance and continuous model monitoring [4], [5], [7], [8].

V. RESEARCH METHODOLOGY

A. Objective

The main objective is to examine the impact of Artificial Intelligence on financial fraud detection and risk management in modern businesses. Specific objectives are: to understand the role of AI in fraud detection; to examine the role of Machine Learning and related technologies; to study AI applications in financial risk management; to identify benefits; to analyse implementation challenges; to examine the connection between fraud detection and broader risk management; and to provide practical suggestions.

B. Research Questions

The study addresses the following questions: How does AI help businesses detect financial fraud? How does AI contribute to financial risk management? What are the major benefits of AI-based detection? What challenges arise during implementation? How should businesses balance automation and human judgement?

C. Research Design

The study uses a descriptive and analytical research design. The descriptive approach explains concepts, applications and challenges, while the analytical approach interprets existing research and identifies implications for modern businesses.

D. Data Sources

The research uses secondary data from academic research papers, peer-reviewed journals, institutional publications, financial-sector reports and other reliable sources. No primary survey or interview has been conducted.

E. Scope

The study covers financial fraud detection, transaction monitoring, credit risk, operational risk, fraud risk, predictive analytics, Machine Learning, Deep Learning, AI governance and financial decision support.

F. Limitations

The research is based on secondary data and does not measure the performance of one specific company. AI technology changes rapidly, and the effectiveness of models depends on data quality. Different industries also face different regulatory and technological conditions. AI may generate

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 10, NCREHAASTE - 2026

false positives or false negatives, and implementation may require substantial resources.

VI. AI IN FINANCIAL FRAUD DETECTION

A. Pattern Recognition

AI can compare current transactions with historical behaviour and identify patterns associated with suspicious activity. Pattern recognition is particularly useful when many variables influence transaction risk.

B. Anomaly Detection

Anomaly detection identifies activity that differs from expected behaviour. Examples include unusual transaction frequency, unexpected geographic activity, unusual amounts or changes in account behaviour.

C. Real-Time Monitoring

Real-time monitoring allows businesses to analyse transactions as they occur. This can reduce the time between a suspicious event and an investigation.

D. Behavioural Analysis

AI can build a behavioural profile based on historical activity. A transaction can then be assessed in the context of the customer's normal behaviour rather than as an isolated event.

E. Automated Alerts

When the system identifies a potentially risky transaction, it can generate an alert. Fraud analysts can then prioritise cases according to risk level.

F. Continuous Improvement

Machine Learning systems can be updated using new and properly labelled information. This can help organisations respond to changing fraud patterns.

TABLE II
MACHINE LEARNING ARCHITECTURES IN FINANCIAL FRAUD DETECTION

ML/DL Paradigm	Core Algorithms	Primary Operational Utility	Operational Limitation
Supervised Learning	XGBoost, LightGBM, Random Forest	Real-time payment scoring, chargeback prediction, pattern classification.	Susceptible to concept drift; requires extensive labelled training records.
Unsupervised Learning	Isolation Forest, One-Class SVM, LOF	Zero-day anomaly detection, discovering atypical transactional clusters.	Generates higher false-positive rates; harder to explain to compliance auditors.
Deep Learning	Recurrent Neural Networks (RNN), LSTM	Time-series transaction velocity, mobile app session behavioral analysis.	High computational demand; requires high-throughput inference hardware.
Graph Neural Networks	Graph Convolutional Networks (GCN)	Uncovering mule networks and circular laundering paths across entities.	Demands large memory footprint and complex graph data pipelines.

VII. ROLE OF MACHINE LEARNING IN FRAUD DETECTION

A. Supervised Learning

Supervised learning uses historical examples labelled as fraudulent or legitimate. The model learns from these examples and applies the learned patterns to new transactions. Its performance depends strongly on the quality and representativeness of training data.

B. Unsupervised Learning

Unsupervised learning identifies unusual patterns without requiring every transaction to have a fraud label. It can be useful for identifying new forms of suspicious activity.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 10, NCREHAASTE - 2026

C. Semi-Supervised Learning

Semi-supervised approaches use a combination of labelled and unlabelled data. This is relevant because confirmed fraud cases are usually much fewer than legitimate transactions.

D. Classification

Classification models can assign transactions to categories such as low risk, high risk, legitimate or potentially fraudulent. Such classification can help investigators prioritise cases.

E. Risk Scoring

AI can generate a risk score based on multiple transaction and behavioural variables. Higher-risk cases can receive additional investigation. No single machine-learning method is suitable for every organisation. Model selection should depend on business objectives, available data, required transparency, technical resources and regulatory considerations.

VIII. AI AND FINANCIAL RISK MANAGEMENT

Financial risk management involves identifying, assessing, monitoring and controlling risks that may affect an organisation's financial objectives. AI can support these activities by analysing historical and real-time information.

A. Credit Risk

AI can analyse repayment history, transaction behaviour and other relevant information to support credit-risk assessment. Predictive models may help identify customers who have a higher probability of default.

B. Market Risk

AI can analyse market information and historical patterns to support monitoring of changes in prices, interest rates and other financial variables.

C. Liquidity Risk

Predictive analytics can assist organisations in analysing cash-flow patterns and identifying potential liquidity pressures before they become severe.

D. Operational Risk

AI can identify unusual patterns in internal processes and systems. This can support early detection of operational problems.

E. Fraud Risk

Fraud risk is closely connected to financial risk. AI-based transaction monitoring can provide early warnings and support risk-based investigations.

TABLE III
STRUCTURAL COMPARISON: TRADITIONAL RULE-BASED VS. MODERN AI SYSTEMS

System Attribute	Traditional Rule-Based Frameworks	Modern AI/ML Fraud Engines
Operational Logic	Static boolean rules (e.g., IF Amount > Threshold THEN Flag).	Probabilistic modeling across multi-dimensional feature vectors.
Adaptability	Requires manual adjustments; slow to respond to changing attacks.	Continuously learns from incoming transactional data streams.
Inference Latency	Batch processing or basic instant lookups; can cause bottlenecks.	Sub-200 millisecond evaluation suitable for real-time clearance.
Data Imbalance Handling	Poor; generates high volumes of false positive alerts.	Employs SMOTE, focal loss, and cost-sensitive classification models.
Explainability & Audit	Clear, straightforward rule trails for auditors.	Requires explainability frameworks such as SHAP and LIME.
Operational Cost	Lower initial software costs, but high ongoing manual review	Higher initial development setup, balanced by reduced manual

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 10, NCREHAASTE - 2026

expenses.	workloads.

IX. RELATIONSHIP BETWEEN FRAUD DETECTION AND RISK MANAGEMENT

Fraud detection should not be treated as an isolated activity. A fraudulent transaction can create financial loss, operational disruption, legal exposure, regulatory consequences and reputational damage.

Risk Management Process Flow:
Suspicious Transaction → AI Alert → Investigation → Risk Assessment → Corrective Action → Monitoring → Risk Reduction

AI can contribute at several stages. It can identify suspicious behaviour, prioritise alerts and provide information to investigators. Once a case is confirmed, the organisation can update controls and risk assessments.

This connection changes the role of fraud detection. Instead of viewing fraud only as an event that must be investigated after it occurs, organisations can use fraud indicators as information for broader risk management. For example, repeated suspicious activity associated with a particular process may indicate a weakness in internal controls. Similarly, unusual activity across related accounts may indicate a wider risk that requires management attention.

The integration of fraud detection and risk management can therefore improve organisational resilience. However, integration should be accompanied by clear accountability and secure information-sharing processes.

X. ANALYSIS AND INTERPRETATION

The analysis of existing research indicates that AI offers significant potential for improving the efficiency and scalability of financial fraud detection. Traditional systems remain valuable because rules are often transparent and easy to audit, but AI can complement these methods by identifying patterns beyond predefined thresholds.

A. Traditional vs AI-Based Detection

Traditional systems generally depend on fixed rules, while AI systems can learn patterns from data. Traditional methods may be easier to explain but can be less adaptable. AI can process larger datasets and support continuous monitoring, but it can be more complex and may produce false alerts. AI should therefore not automatically replace traditional controls. A combined approach can use established rules for known risks and AI models for complex or emerging patterns.

B. AI Applications in Risk Management

AI can support fraud risk, credit risk, market risk, liquidity risk, operational risk and cyber-related risk. Its value increases when information from different business systems can be integrated securely. Interpretation of the literature suggests that the strongest benefits occur when AI is embedded within a complete risk-management process rather than operated as a stand-alone fraud tool.

XI. IMPACT OF AI ON BUSINESS PERFORMANCE

A. Reduction in Potential Losses

Early identification of suspicious activity can allow businesses to investigate transactions before losses become larger. The actual financial effect depends on the quality of controls and the organisation's response.

B. Operational Efficiency

Automating routine screening can reduce the manual workload of employees. Investigators can concentrate on complex cases that require professional judgement.

C. Better Decision-Making

AI-generated risk indicators can provide managers with additional information for financial decisions. This can support prioritisation and resource allocation.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 10, NCREHAASTE - 2026

D. Customer Protection

Fraud monitoring can help protect customers from unauthorised financial activity. Faster identification can also improve the response to incidents.

E. Reputation

Strong fraud controls can support customer confidence. Conversely, a major fraud event can damage trust even when an organisation has sophisticated technology.

XII. CHALLENGES OF AI IN FINANCIAL FRAUD DETECTION

While AI offers substantial capabilities, organisations face several practical challenges during implementation:

- **Data Quality:** AI models depend on reliable and representative data. Missing, incorrect or outdated data can reduce performance.
- **Data Privacy:** Financial data can contain sensitive personal and business information. Organisations must apply appropriate privacy and access controls.
- **Cybersecurity:** AI systems and their data may themselves become targets for cyberattacks. Security must therefore be built into system design.
- **False Positives:** A legitimate transaction may be incorrectly flagged. Too many false alerts can increase investigation costs and inconvenience customers.
- **False Negatives:** An actual fraudulent transaction may sometimes be missed. This can result in financial and reputational loss.
- **Explainability:** Complex models may be difficult to understand. Explainability is important when decisions have significant financial consequences.
- **Algorithmic Bias:** Biased historical data can influence model outputs. Organisations should test models for unfair outcomes.
- **Cost and Skills:** AI adoption may require investment in technology, data infrastructure and skilled professionals.
- **Changing Fraud:** Fraudsters adapt their methods. Models must therefore be monitored and updated continuously.

XIII. ETHICAL AND REGULATORY CONSIDERATIONS

Financial AI requires responsible governance because automated or AI-supported decisions can affect customers, businesses and financial stability.

Transparency is important. Organisations should understand what a model is designed to do, what data it uses and what its limitations are. Where practical, important outputs should be explainable to decision-makers.

Privacy is another key concern. Businesses should use financial information appropriately, restrict access and apply security measures. Data should not be collected or processed without a legitimate business purpose.

Fairness should also be monitored. If historical data contain systematic bias, the model may reproduce that bias. Regular testing can help identify unexpected differences in outcomes.

Accountability must remain clear. An AI system should not become an excuse for unclear responsibility. Organisations should define who monitors the model, who investigates alerts and who makes final high-impact decisions.

Regulatory requirements may differ across countries and industries. Businesses should therefore ensure that AI-based financial processes remain consistent with applicable legal and regulatory obligations.

XIV. HUMAN ROLE IN AI-BASED FINANCIAL MANAGEMENT

AI is powerful at processing data, but human professionals remain important. Fraud investigations can involve context, intent and unusual circumstances that may not be fully represented in a dataset.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 10, NCREHAASTE - 2026

AI can perform routine screening, identify patterns and prioritise cases. Human analysts can then examine high-risk alerts, collect additional information and decide whether an action is appropriate.

Human oversight is particularly important when an AI decision could significantly affect a customer or a business relationship. Employees should be able to question, review and escalate model outputs.

The most effective approach is therefore likely to be human-AI collaboration. Employees should understand enough about the model to interpret its output, recognise limitations and identify unusual cases.

XV. FUTURE SCOPE OF AI IN FINANCIAL FRAUD DETECTION

Looking forward, key developments in financial fraud detection will include:

- **Explainable AI (XAI):** Greater emphasis on explaining why a transaction or customer has been classified as risky.
- **Real-Time AI:** Sub-second scoring reducing delay between suspicious events and automated mitigation.
- **Generative AI:** Assisting fraud teams with case summaries, forensic documentation, and simulated stress-testing.
- **Graph-Based Detection:** Tracing entity links, device fingerprints, and hidden transaction networks across banking rails.
- **Integrated Risk Platforms:** Merging fraud prevention, credit risk, liquidity analysis, and regulatory reporting into unified systems.
- **Continuous Learning:** Real-time streaming evaluation to counter concept drift and emerging attack strategies.

XVI. FINDINGS AND SUGGESTIONS

A. Findings

The study finds that AI has significant potential to improve financial fraud detection and risk management. Machine Learning can identify suspicious patterns in large datasets, while AI-based monitoring can provide faster alerts. AI can also support credit assessment, operational risk monitoring, liquidity analysis and other financial activities.

The findings also show that AI is not automatically superior in every situation. Traditional rules can remain useful because they are transparent and effective for known patterns. The strongest approach combines traditional controls with AI-based analytics. Data quality is a major determinant of AI performance. Privacy, cybersecurity, explainability, fairness, false alerts, implementation costs and shortage of skilled professionals are important challenges.

B. Suggestions

Businesses should adopt AI gradually and begin with clearly defined use cases. They should maintain high-quality data, establish strong cybersecurity and regularly evaluate model performance. Human experts should supervise important financial decisions. Employees should receive training in AI, fraud investigation, data interpretation and financial controls.

Organisations should create clear AI governance policies covering accountability, privacy, model monitoring, fairness and security. Models should be tested regularly and updated as fraud techniques change. Businesses should also measure AI performance using appropriate indicators, including detection effectiveness, false-alert levels, investigation time and operational impact.

XVII. CONCLUSION

Artificial Intelligence is transforming the way modern businesses approach financial fraud detection and risk management. The growth of digital transactions has increased both the volume of financial information and the opportunities for

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 10, NCREHAASTE - 2026

sophisticated fraud. AI provides tools for pattern recognition, anomaly detection, real-time monitoring, predictive analysis and automated risk scoring.

The study concludes that AI can improve the speed, scalability and analytical capability of financial fraud detection. It can also contribute to proactive risk management by helping businesses identify potential threats earlier and prioritise management attention. However, AI does not remove the need for human expertise. Data quality, privacy, cybersecurity, explainability, fairness and model governance remain critical. Businesses should therefore adopt a balanced human-AI approach. Responsible implementation, continuous monitoring and strong internal controls can help organisations obtain the benefits of AI while managing its limitations.

AI is therefore not only a technological solution but also an important support system for financial management. Its ability to analyse large volumes of transactional and behavioural data can help organisations recognise suspicious activities that may be difficult to identify through conventional rule-based methods alone. When AI is integrated with real-time monitoring, risk scoring and automated alerts, businesses can respond to potential threats more quickly and allocate investigation resources according to the level of risk.

The study also shows that effective AI depends on reliable data, appropriate model design and responsible use of results. Poor-quality data can reduce accuracy, while false positives and false negatives can affect both investigation costs and fraud losses. Therefore, regular testing, model validation and continuous monitoring are necessary as fraud techniques change. AI should also be connected with internal controls, cybersecurity, employee awareness and clear governance. Human experts remain important for reviewing complex cases and making high-impact decisions. Overall, a balanced human-AI approach can make fraud detection faster, more scalable and more proactive while supporting responsible and resilient financial management.

REFERENCES

[1] S. Ahmed, M. M. Alshater, A. E. Ammari, and H. Hammami, "Artificial intelligence and machine learning in finance: A bibliometric review," Research in International Business and Finance, vol. 61, p. 101646, 2022.

[2] Bank for International Settlements, "Regulating AI in the financial sector: Recent developments and main challenges," FSI Insights on Financial Regulation, Paper No. 58, pp. 1-34, 2024.

[3] P. Giudici, M. Centurelli, and S. Turchetta, "Artificial intelligence risk measurement," Expert Systems with Applications, vol. 235, p. 121220, 2024.

[4] Indian Cyber Crime Coordination Centre (I4C), Annual Compendium on Cyber Financial Crimes and Preventive Frameworks, Ministry of Home Affairs, Government of India, 2024.

[5] National Payments Corporation of India (NPCI), UPI Procedural Guidelines and Operational Risk Controls, Technical Documentation Series, Mumbai, 2024.

[6] R. Patel and S. Kumar, "Comparative analysis of machine learning algorithms and data balancing techniques for credit card fraud detection," Procedia Computer Science, vol. 245, pp. 677-688, 2024.

[7] Reserve Bank of India (RBI), Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices, RBI/2023-24/107, Department of Regulation, Central Office, Mumbai, 2023.

[8] Reserve Bank of India (RBI), Report on Currency and Finance (RCF): Digitalisation, Financial Innovation and Systemic Resilience, Reserve Bank of India, Mumbai, 2024.

[9] J. K. Roy and L. Vasa, "Machine learning and artificial intelligence methods for FinTech credit scoring and risk management," International Journal of Business Analytics, vol. 11, no. 1, pp. 1-18, 2024.

[10] M. Sharma and T. Becker, "The role of artificial intelligence in preventing corporate crime," Journal of Economic Criminology, vol. 5, p. 100091, 2024.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)