International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 04 April-2026 | Impact Factor: 3.5

AI-Based Fraud Detection Systems in Banking and their Effect on Financial Risk Management

Submitted By

Kunal Kumar Singh

Course- (MBA) Sec- A, 4th Sem
Roll No-SM/MB/2401/061 PRF NO- NIU-24-24786
Enrollment Number: 24020272193

Under the Guidance of

Dr. Kalpana Rawat

Assistant Professor School of Business Management

How to Cite this Article:

Singh, K. K. (2026). AI-Based Fraud Detection Systems in Banking and their Effect on Financial Risk Management. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.675

https://doi.org/10.55041/ijcope.v2i4.675

Abstract

The rapid digitization of banking services has significantly increased the risk of financial fraud, including credit card fraud, identity theft, and online transaction fraud .In recent years, financial institutions have increasingly turned to artificial intelligence (AI) to combat fraud and enhance risk management strategies. As the complexity of financial transactions and the sophistication of fraudulent activities grow, traditional rule-based systems become insufficient. AI technologies, particularly machine learning (ML), natural language processing (NLP), and predictive analytics, have proven to be essential in detecting fraudulent activities in real-time, improving the accuracy of risk assessments, and reducing operational costs. This research paper explores the integration of AI in financial transaction fraud detection and risk management, discussing its applications, benefits, challenges, and future prospects. This research investigates the impact of AI technology in banking institutions through its use cases while exploring methodologies together with advantages along with barriers it creates. This research shows that AI-controlled financial systems use data protection methods to minimize losses and produce better decisions with additional needed steps to protect data security and ethical standards.

Keywords:- Artificial Intelligence, Machine Learning, Financial Fraud Detection, Risk Management, Deep Learning, Predictive Analytics, Banking Security.

1 Introduction

The global banking sector is increasingly adopting AI technologies to improve operational efficiency and risk management. Fraud detection has become a major application of AI in banking due to the growing volume of digital transactions. AI systems such as machine learning algorithms, neural networks, and anomaly detection models analyze large datasets to identify suspicious behaviour patterns.

Banks face significant financial losses due to fraudulent transactions, making fraud detection systems critical for financial risk management. AI-based systems provide faster and more accurate identification of fraudulent activities compared to traditional rule-based systems.

Financial institutions face a growing challenge in preventing fraud, managing risks, and ensuring the safety of digital transactions. Fraudulent activities, such as identity theft, account takeover, and money laundering, have become more prevalent with the expansion of digital banking, online shopping, and mobile transactions. Traditional fraud detection systems, often based on static rules, struggle to keep up with the evolving tactics used by fraudsters. AI, with its ability to analyze large volumes of data and recognize complex patterns, is increasingly being leveraged to address these challenges. This paper discusses the role of AI in fraud detection and risk management, examining its applications, advantages, and limitations. Additionally, we explore how AI can enhance the financial industry's ability to identify fraud early, mitigate risks, and comply with regulatory requirements**.**

1.1 Objective of the study

1. To examine the role of Artificial Intelligence in fraud detection and risk management in the banking sector.
2. To analyze the limitations of traditional fraud detection systems and the need for AI-based solutions.
3. To study the applications of AI in fraud detection, such as real-time monitoring, predictive analytics, and anomaly detection.

1.2 Research question

1. How does Artificial Intelligence contribute to fraud detection in the banking sector?
2. What are the key limitations of traditional fraud detection systems compared to AI-based approaches?
3. What are the major applications of AI in fraud detection and risk management?
4. How does AI improve the accuracy and efficiency of fraud detection systems?

1.2 Hypotheses

H1: Artificial Intelligence has a significant positive impact on fraud detection effectiveness in the banking sector.
H2: AI-based fraud detection systems are more accurate than traditional rule-based systems.
H3: The use of AI significantly reduces false positives in fraud detection.
H4: Artificial Intelligence improves the efficiency and speed of fraud detection processes.
H0: AI-based systems enhance financial risk management and decision-making in banks.

2 Literature Review

The increasing use of digital banking and online transactions has led to a significant rise in financial fraud, making traditional detection methods less effective. As a result, Artificial Intelligence (AI) has emerged as a powerful tool in enhancing fraud detection and financial risk management in the banking sector.

Rohit Raj (2022) highlighted that financial fraud has become more complex and widespread in the digital era. The study emphasized that AI technologies such as machine learning and big data analytics help in analyzing large volumes of transaction data, detecting unusual patterns, and improving fraud detection accuracy. It also pointed out

the shift from traditional fraud to cyber- enabled fraud, where AI enables real-time monitoring and better risk management.

Similarly, Oluwabusayo Adijat Bello (2024) explained that AI plays a crucial role in modern fraud prevention through techniques like machine learning, deep learning, and natural language processing. These technologies improve efficiency, reduce false positives, and support real-time decision-making. However, challenges such as data privacy and high implementation costs remain key concerns.

Adhikari, Hamal, and Jnr (2024) found that AI-based systems are more effective than traditional methods due to their scalability, adaptability, and ability to process large datasets in real time. Supporting this, Mehrotra et al. (2024) emphasized that AI enhances fraud detection speed and accuracy while reducing financial losses, although issues like data quality and implementation costs still exist.

Nweze et al. (2024) highlighted that AI and machine learning not only improve fraud detection but also strengthen financial risk management by providing predictive insights and real-time analysis.

Prakash and Sharma (2024) further stated that AI-driven systems improve security by detecting anomalies and ensuring safer financial transactions, thereby increasing customer trust.

In addition, Paul and Darden (2025) emphasized that AI supports regulatory compliance and enhances transparency in financial systems. Yaseen and Al-Amarneh (2025) focused on ethical considerations, stressing the importance of trust, fairness, and transparency in AI adoption in banking.

Odufisan et al. (2025) discussed the use of supervised, unsupervised, and deep learning techniques in fraud detection, concluding that these methods significantly improve efficiency in the digital economy. Earlier research by Chandola et al. (2009) highlighted the importance of anomaly detection techniques in identifying unknown and emerging fraud patterns.

Overall, the literature indicates that AI-based fraud detection systems are more efficient, accurate, and scalable than traditional methods. They enable real-time monitoring, reduce financial losses, and improve financial risk management. However, challenges such as data privacy, high implementation costs, and ethical concerns remain important issues that need to be addressed.

3.1 Research Design

The present study is conducted in Dankaur, Uttar Pradesh. The data for this research has been collected from banking professionals, IT experts, risk managers, and FinTech specialists working in and around this area.

Dankaur has been selected as the study area due to the growing use of digital banking services and increasing adoption of Artificial Intelligence in financial operations. This makes it suitable for analyzing the impact of AI-based fraud detection systems on financial risk management.

The analytical component, on the other hand, evaluates the relationship between AI-based fraud detection systems and financial risk management outcomes such as accuracy, efficiency, and risk reduction. This approach enables the researcher to draw meaningful conclusions regarding the effectiveness of AI in improving banking security and decision-making processes.

3.2 Research Approach

This study is based on a mixed research approach, combining both quantitative and qualitative methods to provide a comprehensive and balanced analysis.

Quantitative Approach

The quantitative method involves the collection of numerical data through structured questionnaires. This data is analyzed using statistical tools to measure relationships, patterns, and the level of impact of AI on fraud detection and risk management.

1. Survey questionnaires are used to collect responses
2. Statistical techniques are applied for data interpretation

Qualitative Approach

The qualitative method is used to gain deeper insights into the practical implementation and challenges of AI systems in banking.

Interviews with banking professionals provide expert opinions

Secondary sources such as reports and case studies help in understanding real-world applications

This combined approach enhances the reliability and depth of the study by integrating numerical analysis with practical insights.

3.3 Data Sources

Primary Data

Primary data is collected directly from respondents through a structured questionnaire. The respondents include professionals who are actively involved in banking operations and have knowledge of AI and fraud detection systems.

The target respondents include:

- Bank employees
- Risk management professionals
- IT professionals in the banking sector
- FinTech experts

This ensures that the data collected is relevant, practical, and based on real industry experience.

Secondary Data

Secondary data is collected from various reliable and published sources to support and validate the research findings.

These sources include:

- Annual reports of banks
- Academic research journals
- Reports published by the Reserve Bank of India (RBI)

- Industry publications and articles
- Financial and statistical databases

Secondary data helps in building theoretical understanding and supporting the analysis of primary data.

3.4 Sampling Design

Population

The population of the study consists of employees and professionals working in the banking and financial sector in India, particularly those involved in fraud detection and risk management.

Sample Size

A sample size of **100 to 150 respondents** is selected for the study. This sample size is considered adequate to obtain reliable and meaningful results within the scope of the research.

Sampling Technique

The study uses purposive sampling, a non-probability sampling technique where respondents are selected based on their knowledge, expertise, and involvement in the subject area.

This method ensures that only relevant and informed participants contribute to the research.

Sample Distribution

Respondent Category	Number of Respondents
Risk Managers	30
IT Professional	30
Bank officers	40
Fintech Expert	20
Total	120

This distribution ensures a balanced representation of different professional perspectives.

3.5 Data Collection Instrument

The primary data is collected using a structured questionnaire designed on a 5-point Likert scale to measure the level of agreement among respondents.

Questionnaire Design

The questionnaire consists of statements related to AI-based fraud detection and financial risk management.

Sample Statements:

- AI improves fraud detection accuracy in banking

- AI systems reduce financial losses caused by fraud
- AI-based systems enable faster detection of suspicious transactions
- AI enhances overall financial risk management

Measurement Scale:

- 1 = Strongly Disagree
- 2 = Disagree
- 3 = Neutral
- 4 = Agree
- 5 = Strongly Agree

The Likert scale helps in quantifying respondents' opinions and facilitates statistical analysis.

3.6 Variables of the Study

The study includes both independent and dependent variables to analyze their relationship.

Independent Variables	**Independent Variables**
AI Fraud Detection Systems	Financial Risk Management
Machine Learning Algorithms	Fraud Detection Systems
Data Analytics	Risk Reduction

The independent variables represent AI-related technologies, while the dependent variables reflect outcomes related to risk management and fraud detection performance.

3.7 Data Analysis Tools

The collected data is analyzed using various statistical techniques to derive meaningful insights.

Statistical Tools Used:

Descriptive Statistics – to summarize and present data

Correlation Analysis – to measure relationships between variables **Regression Analysis** – to examine the impact of AI on risk management **Factor Analysis** – to identify underlying factors
Hypothesis Testing (t-test and ANOVA) – to test research hypotheses

Software Tools:

SPSS (Statistical Package for Social Sciences) Microsoft Excel
Python (optional for advanced analysis)

These tools help in ensuring accuracy, reliability, and proper interpretation of data.

3.8 Reliability and Validity

Reliability

Reliability refers to the consistency of the research instrument. In this study, Cronbach's Alpha is used to measure the internal consistency of the questionnaire. A higher value of Cronbach's Alpha indicates that the data collected is reliable.Validity

Validity ensures that the research measures what it is intended to measure. Content validity is ensured through expert review and academic guidance

The questionnaire is designed based on research objectives and literature This ensures that the results of the study are accurate and meaningful.

4 Data Analysis and Interpretation

This chapter presents the analysis and interpretation of data collected from respondents regarding the impact of Artificial Intelligence (AI)-based fraud detection systems on financial risk management in the banking sector. The data has been collected through a structured questionnaire using a 5-point Likert scale from a sample of banking professionals, including risk managers, IT professionals, bank officers, and FinTech experts. The data for this study has been collected from respondents located in Dankaur, Uttar Pradesh.

The analysis is conducted using statistical tools such as descriptive statistics, correlation, and regression analysis, as defined in the research methodology. The objective of this chapter is to examine the relationship between AI adoption and key outcomes such as fraud detection accuracy, risk reduction, and financial performance

4.1 Demographic Profile of Respondents

The study includes a total of 120 respondents, selected using purposive sampling, as per the research design.

Table 4.1: Distribution of Respondents

Respondent Category	**Number of Respondents**	**Percentage**
Risk Managers	30	25%
IT Professionals	30	25%
Bank Officers	40	33.33%
Fin Tech Expert	20	16.67%
Total	**120**	**100%**

Interpretation:

The data shows that the highest proportion of respondents are bank officers (33.33%), followed by risk managers and IT professionals (25% each). FinTech experts account for 16.67% of the sample.

This distribution ensures that the study reflects diverse professional insights related to AI implementation and risk management.

4.2 Descriptive Statistics Analysis

Descriptive statistics are used to analyze the responses collected through the Likert-scale questionnaire. The analysis focuses on key variables such as AI effectiveness, fraud detection accuracy, and financial risk management

Table 4.2: AI Improves Fraud Detection Accuracy

Response	Frequency	Percentage
Strongly Agree	48	40%
Agree	44	36.67%
Neutral	14	11.67%
Disagree	8	6.67%
Strongly Disagree	6	5%

Interpretation:

A majority of respondents (76.67%) either agree or strongly agree that AI improves fraud detection accuracy. This indicates strong acceptance of AI technologies in identifying fraudulent activities.

Table 4.3: AI Reduces Financial Losses Due to Fraud

Response	Frequency	Percentage
Strongly Agree	45	37.5%
Agree	42	35%
Neutral	18	15%
Disagree	9	7.5%
Strongly Disagree	6	5%

Interpretation:

Approximately 72.5% of respondents agree that AI helps in reducing financial losses, highlighting its importance in financial risk mitigation.

Table 4.4: AI Detects Suspicious Transactions Faster

Response	Frequency	Percentage
Strongly Agree	50	41.67%
Agree	43	35.83%
Neutral	12	10%
Disagree	9	7.5%
Strongly Disagree	6	5%

Interpretation:

More than 77% of respondents believe that AI enables faster detection of suspicious transactions, emphasizing its role in real-time fraud prevention.

Table 4.5: AI Improves Financial Risk Management

Response	Frequency	Percentage
Strongly Agree	47	39.17%
Agree	45	37.5%
Neutral	15	12.5%
Disagree	7	5.83%
Strongly Disagree	6	5%

Interpretation:

A significant majority (76.67%) agree that AI enhances financial risk management, indicating its effectiveness in improving decision-making and risk control.

Table 4.6: Correlation Results

Variables	Correlation coefficient (r)
AI Systems & Fraud Detection Accuracy	0.71
AI Systems & Risk Reduction	0.69
Data Analytics & Financial Management	0.73

Interpretation:

The correlation values indicate a strong positive relationship between AI technologies and financial risk management variables. This means that higher adoption of AI leads to improved fraud detection and better risk control.

4.3 Regression Analysis

Regression analysis is used to measure the impact of AI on financial risk management.

Model Summary:

- $R^2 = 0.64$
- Adjusted $R^2 = 0.61$
- p-value < 0.05

Interpretation:

The R^2 value of 0.64 indicates that 64% of the variation in financial risk management is explained by AI-based fraud detection systems. The significance level ($p < 0.05$) confirms that the relationship is statistically significant.

This demonstrates that AI plays a crucial role in enhancing financial risk management in the banking sector.

Hypothesis Testing

Based on the regression analysis, the significance value (p-value) is less than 0.05, indicating that the results are statistically significant. Therefore, the null hypotheses (H_{01} to H_{05}) are rejected, and the alternative hypotheses (H_1 to H_5) are accepted.

The strong positive correlation values (r = 0.69 to 0.73) and the majority agreement of respondents (above 70%) further support the acceptance of all alternative hypotheses. This confirms that Artificial Intelligence has a significant positive impact on fraud detection and financial risk management in the banking sector.

4.4 Key Findings

Based on the above analysis, the study reveals the following findings:

- AI significantly improves fraud detection accuracy in banking operations
- AI helps in reducing financial losses caused by fraudulent activities
- AI enables faster identification of suspicious transactions

There is a strong positive relationship between AI adoption and financial risk management

- AI enhances efficiency, decision-making, and overall risk control mechanisms

5 Conclusion

The present study examined the role of Artificial Intelligence (AI)-based fraud detection systems and their impact on financial risk management in the banking sector. With the rapid growth of digital banking and online financial transactions, the risk of fraud has increased significantly, making it essential for banks to adopt advanced technological solutions.

The findings of the study clearly indicate that AI-based systems significantly enhance the efficiency and accuracy of fraud detection. These systems are capable of analyzing large volumes of transaction data, identifying abnormal patterns, and detecting fraudulent activities in real time. As a result, banks are able to reduce financial losses and improve operational efficiency.

Moreover, AI technologies support proactive risk management by enabling early identification of potential threats. This allows financial institutions to take preventive measures rather than reacting

after fraud has occurred. Overall, the study concludes that AI plays a crucial role in strengthening financial risk management and ensuring the security of modern banking systems.

5.1 Recommendations

Based on the findings of the study, the following recommendations are suggested:

1. **Adoption of Advanced AI Technologies**

Banks should increase their investment in AI-based fraud detection systems to enhance their ability to detect and prevent financial fraud.

2. **Integration with Emerging Technologies**

The integration of AI with technologies such as blockchain can further improve transparency, security, and fraud prevention mechanisms in banking systems.

3. **Employee Training and Development**

Continuous training programs should be conducted to equip banking professionals with the necessary skills to effectively use AI tools and systems.

4. **Regulatory Support and Framework**

Regulatory authorities should establish clear guidelines and policies for the implementation of AI in banking to ensure ethical use, data protection, and system reliability.

5. **Continuous Monitoring and System Upgradation**

Banks should regularly update and monitor their AI systems to keep up with evolving fraud techniques and technological advancements.

5.2 Limitations of the Study

Despite its contributions, the study has certain limitations:

- The study is based on a limited sample size, which may not fully represent the entire banking sector.
- The research relies on survey-based responses, which may be subject to personal bias or perception errors.
- The study focuses mainly on the banking sector, limiting its applicability to other financial domains.
- The rapid evolution of AI technologies may result in new developments that are not covered in this study.

5.3 Future Scope of the Study

The study provides a foundation for future research in the field of AI and financial fraud detection. The following areas can be explored further:

- **Application of Deep Learning Models**

Future research can focus on advanced deep learning techniques such as neural networks and LSTM models for improved fraud detection accuracy.

- **Fraud Detection in Cryptocurrency Transactions**

With the rise of digital currencies, future studies can explore AI-based fraud detection in cryptocurrency and blockchain-based systems.

- **AI in FinTech Risk Management**

Further research can examine the role of AI in managing financial risks within FinTech companies.

- **Real-Time Fraud Detection Systems**

Future studies can focus on enhancing real-time fraud detection using streaming data and advanced analytics.

- **Hybrid AI Models**

Combining machine learning, deep learning, and blockchain technologies can be explored to develop more robust and efficient fraud detection systems.

Bibliography

Journal Articles

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. Bahnsen, A. C., Aouada, D., Stojanovic, A., & Ottersten, B. (2016). *Feature engineering strategies for credit card fraud detection*. **Expert Systems with Applications**, 51, 134–142.

3. Dal Pozzolo, A., Caelen, O., Le Borgne, Y. A., Waterschoot, S., & Bontempi, G. (2014). *Learned lessons in credit card fraud detection from a practitioner perspective*. **Expert Systems with Applications**, 41(10), 4915–4928.

4. Chen, C., Li, C., & Huang, J. (2018). *Fraud detection using machine learning and deep learning*. **IEEE Access**, 6, 72950–72963.

5. Abdallah, A., Maarof, M. A., & Zainal, A. (2016). *Fraud detection system: A survey*. **Journal of Network and Computer Applications**, 68, 90–113.

Artificial Intelligence & Machine Learning Foundations

6. Deep Learning – Ian Goodfellow, Yoshua Bengio, & Aaron Courville (2016). MIT Press.

7. Pattern Recognition and Machine Learning – Christopher M. Bishop (2006). Springer.

8. Artificial Intelligence a Modern Approach – Stuart Russell & Peter Norvig (4th ed.). Pearson.

Recent Research & Reviews

9. Hafez, I. Y., Hafez, A. Y., Saleh, A., & Abd El-Mageed, A. A. (2024). *A systematic review of AI- enhanced techniques in credit card fraud detection*. **Journal of Big Data**, 11, Article 48.

10. Yang, H., Shukur, Z., & Sahran, S. (2023). *Artificial intelligence approaches for financial fraud detection: A review*. **Applied Sciences**, 13(4), 1931.

11. Fiore, U., De Santis, A., Perla, F., Zanetti, P., & Palmieri, F. (2019). *Using generative adversarial networks for improving classification effectiveness in credit card fraud detection*. **Information Sciences**, 479, 448–455.

12. Carcillo, F., Dal Pozzolo, A., Le Borgne, Y. A., Caelen, O., Mazzer, Y., & Bontempi, G. (2019). *Scarff: A scalable framework for streaming credit card fraud detection with Spark*. **Information Fusion**, 41, 182–194.

Financial Risk Management & Banking Context

13. Jurgovsky, J., Granitzer, M., Ziegler, K., et al. (2018). *Sequence classification for credit-card fraud detection*. Expert Systems with Applications, 100, 234–245.

14.West, J., & Bhattacharya, M. (2016). *Intelligent financial fraud detection: A comprehensive review*. Computers & Security, 57, 47–66.

15.Hand, D. J., & Whitrow, C. (2008). *Statistical challenges of fraud detection in banking*. Statistica**l Science**, 23(3), 353–368.

Conference Papers

16.Whitrow, C., Hand, D. J., Juszczak, P., Weston, D., & Adams, N. (2009). *Transaction aggregation as a strategy for credit card fraud detection*. In Proceedings of IEEE International Conference on Data Mining, 1215–1220.

17.Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). *A comprehensive survey of data mining-based fraud detection research*. In ACM SIGKDD Explorations Newsletter, 12(2), 1–14.

Industry Reports & Practical Insights

18.McKinsey & Company (2020). *The use of AI in risk management in banking*.

19.Deloitte (2021). *AI and financial crime detection in banking sector*.

20.PwC (2022). *Global Economic Crime and Fraud Survey*.