

**ARTIFICIAL INTELLIGENCE IN CREDIT CARD FRAUD DETECTION: A
SYSTEMATIC LITERATURE REVIEW****Mrs. Kousarziya**

Assistant Professor, Department of Commerce

Vidyavahini First Grade College Tumkur Tumkur, -572103, India

Email: kousarziya05@gmail.com**Mr. Anand Chandrasekaran**

Director, Information Technology

Fiserv India Pvt. Ltd.

Email: kcsanand@gmail.com**Ms. Devika M S**

Assistant Professor, Department of Commerce,

Acharya Institute of Graduate Studies, Soladevanahalli, Bengaluru-560107

Email: devikams1999@gmail.com**Mrs. Razia Kousar**

Assistant Professor, Department of Commerce & Management

SSCACs Tumkur, Karnataka , 572101, India

Email: raziakousar436@gmail.com

ABSTRACT:

The rapid expansion of digital payment systems has revolutionized financial transactions, but it has also increased the frequency and sophistication of credit card fraud. As fraudsters continue to adopt advanced techniques, traditional rule-based fraud detection systems often struggle to identify fraudulent activities in real time, resulting in delayed detection, higher false-positive rates, and financial losses for both financial institutions and customers. In response to these challenges, Artificial Intelligence (AI) has emerged as a transformative technology capable of enhancing fraud detection through machine learning, predictive analytics, anomaly detection, and real-time transaction monitoring.

This descriptive study examines the role of Artificial Intelligence in strengthening credit card fraud detection within the banking sector. Drawing on secondary data from published research articles, industry reports, banking publications, and government documents, the study reviews the evolution of AI-driven fraud detection systems and their contribution to improving transaction security. It explores the application of key AI techniques, including machine learning, predictive analytics, anomaly detection, and automated decision-making, in identifying fraudulent transaction patterns and supporting timely intervention.

The review indicates that AI-enabled fraud detection systems offer significant advantages over conventional approaches by improving detection accuracy, reducing false-positive alerts, enabling real-time monitoring, and enhancing the overall security of digital payment systems. The study also highlights the challenges associated with AI implementation, including data privacy, algorithm transparency, infrastructure requirements, and evolving cyber threats. The findings provide valuable insights for banks, fintech companies, regulators, and policymakers seeking to strengthen fraud prevention strategies and build secure, resilient, and customer-centric digital financial ecosystems.

Keywords:

Artificial Intelligence, Credit Card Fraud Detection, Machine Learning, Banking, Financial Technology, Fraud Prevention, Digital Payments, Financial Security.

INTRODUCTION:

The rapid growth of digital technologies has transformed the way financial transactions are conducted worldwide. Credit cards have become one of the most widely used payment methods due to their convenience, speed, and seamless integration with digital banking and e-commerce platforms. In India, the expansion of digital payment systems, mobile banking, and online shopping has significantly increased credit card usage, supporting the country's vision of a cashless economy. However, this digital transformation has also exposed financial institutions and consumers to an increasing number of cyber threats, particularly credit card fraud.

Over the years, credit card fraud has evolved from simple card theft and counterfeit transactions to sophisticated cybercrimes such as phishing, identity theft, card-not-present (CNP) fraud, account takeover, and synthetic identity fraud. The growing volume of digital transactions and the constantly changing tactics used by fraudsters have made fraud detection a major concern for banks, payment service providers, and fintech companies. Besides financial losses, fraudulent transactions also reduce customer confidence and pose significant challenges to maintaining secure digital payment ecosystems.

Traditionally, banks have relied on rule-based systems to detect suspicious transactions. While these systems are effective in identifying known fraud patterns, they often struggle to detect new and complex fraud techniques in real time. Frequent manual updates, limited adaptability, and a high number of false alerts reduce their effectiveness, highlighting the need for more intelligent and responsive fraud detection mechanisms.

Artificial Intelligence (AI) has emerged as a promising solution to these challenges. Technologies such as machine learning, predictive analytics, anomaly detection, and real-time transaction monitoring enable financial institutions to analyze large volumes of transaction data, recognize unusual customer behavior, and identify potential fraud more accurately and efficiently. Unlike conventional systems, AI continuously learns from new data, allowing it to adapt to evolving fraud patterns and improve detection performance over time.

Today, AI has become an integral part of modern fraud prevention strategies adopted by banks and fintech organizations. Its ability to improve detection accuracy, reduce false-positive alerts, enhance operational efficiency, and strengthen customer trust has made it a valuable tool in securing digital financial transactions. At the same time, issues related to data privacy, ethical AI, algorithm transparency, and regulatory compliance remain important considerations for its successful implementation.

This paper provides a descriptive review of the role of Artificial Intelligence in credit card fraud detection. Drawing on published research, industry reports, and government publications, it examines the evolution of AI-based fraud detection systems, their applications, benefits, challenges, and emerging trends in the banking sector. The study aims to provide a comprehensive understanding of how AI is transforming fraud prevention and offers insights that can support banks, fintech companies, regulators, and policymakers in building safer, more resilient, and customer-centric digital financial ecosystems.

LITERATURE REVIEW:

- Choi, Lee & Kim (2024): The study examined the effectiveness of Artificial Intelligence in detecting fraudulent credit card transactions using deep learning algorithms. The research found that AI-based models significantly improved fraud detection accuracy while reducing false-positive rates compared to conventional rule-based systems. However, the study mainly focused on algorithm performance without examining operational implementation in banking environments. Further research is required to understand AI adoption and its impact on fraud prevention within financial institutions.
- Sharma & Gupta (2023): The study explored the adoption of machine learning techniques for fraud detection in Indian commercial banks. The findings revealed that machine learning algorithms enhanced transaction monitoring by identifying suspicious activities in real time, thereby minimizing financial losses. However, the study primarily emphasized technical implementation and overlooked customer trust and organizational readiness for AI adoption.
- Aslam et al. (2023): The research investigated the role of predictive analytics in financial fraud detection. The results indicated that predictive analytics significantly improved fraud prediction by analyzing historical transaction patterns and identifying abnormal customer behavior. The study suggested that integrating predictive analytics with other AI technologies could further strengthen fraud prevention mechanisms in banking.
- Tang (2022): The study analyzed Artificial Intelligence applications in digital banking security. The findings demonstrated that AI-enabled fraud detection systems reduced response time and improved fraud identification accuracy through real-time transaction monitoring. However, the research focused

on developed economies, leaving limited evidence regarding AI implementation in emerging economies such as India.

- Pandey (2022): The paper examined the role of Artificial Intelligence and blockchain technologies in enhancing financial security. The findings suggested that AI combined with blockchain improves transaction transparency, minimizes fraudulent activities, and strengthens cybersecurity. The study highlighted the need for empirical research assessing AI's practical impact on fraud detection effectiveness in the banking sector.
- Garg & Mehta (2021): The study evaluated the effectiveness of anomaly detection techniques in identifying fraudulent financial transactions. The findings revealed that anomaly detection models successfully recognized unusual transaction patterns before fraud occurred. However, the research was limited to simulation datasets and did not validate the framework using real banking professionals or organizational settings.
- Kumar & Singh (2021): The research examined the influence of Artificial Intelligence on banking risk management. The findings indicated that AI improves operational efficiency by automating fraud detection, reducing manual intervention, and strengthening decision-making processes. The study recommended integrating AI with existing banking infrastructure to improve financial security.
- Bhattacharya et al. (2020): The study focused on customer perceptions of AI-enabled banking services. The findings showed that customers expressed greater confidence in financial institutions employing AI-based fraud prevention systems due to faster detection and improved transaction security. However, the study did not investigate the relationship between AI capabilities and fraud detection performance.
- Ngai et al. (2019): The research reviewed various data mining and machine learning techniques used in financial fraud detection. The findings concluded that supervised learning algorithms achieved higher fraud detection accuracy than traditional statistical approaches. The study emphasized the importance of continuously updating AI models to address evolving fraud patterns.
- Niu (2019): The study investigated machine learning applications in financial fraud analytics. The findings revealed that intelligent algorithms effectively identify fraudulent transaction behavior by learning from large datasets and adapting to changing customer spending patterns. The research suggested integrating real-time analytics to improve fraud detection performance.
- Dal Pozzolo et al. (2018): The study proposed machine learning models for detecting credit card fraud in highly imbalanced datasets. The findings demonstrated that advanced classification techniques significantly improved fraud detection while reducing false alarms. The study mainly concentrated on predictive accuracy rather than practical implementation within banking organizations.
- Carcillo et al. (2018): The paper examined real-time fraud detection using machine learning in payment systems. The findings indicated that continuous monitoring of transactional data substantially enhanced fraud detection capabilities and minimized financial losses. The authors recommended integrating AI with behavioral analytics to improve detection efficiency.
- Jurgovsky et al. (2018): The research explored deep learning techniques for credit card fraud detection using sequential transaction data. The study found that recurrent neural network models outperformed conventional machine learning algorithms in identifying fraudulent transactions. However, computational complexity and implementation costs remained significant challenges.

RESEARCH GAP

Existing studies on Artificial Intelligence (AI) in credit card fraud detection primarily emphasize algorithm development and model accuracy, with limited efforts to consolidate their findings into a comprehensive review. As AI technologies and digital payment systems continue to evolve rapidly, the available literature remains fragmented, making it difficult to understand the broader applications, benefits, challenges, and future potential of AI in fraud prevention. Furthermore, there is a lack of recent review studies that synthesize evidence from academic research, industry practices, and the Indian banking context. This study addresses this gap by providing a comprehensive descriptive review of AI-driven credit card fraud detection, highlighting current advancements, implementation challenges, and emerging trends to support future research and informed decision-making in the banking and fintech sectors.

RESEARCH METHODOLOGY

Research Design

The study adopts a descriptive review research design to examine the role of Artificial Intelligence (AI) in credit card fraud detection. It synthesizes existing literature to provide a comprehensive understanding of AI applications, benefits, challenges, and emerging trends in the banking sector.

Data Sources

The study is based exclusively on secondary data collected from peer-reviewed journal articles, books, conference proceedings, industry reports, and publications from organizations such as the Reserve Bank of India (RBI), National Payments Corporation of India (NPCI), Visa, Mastercard, IBM, Deloitte, and PwC.

Literature Search Strategy

Relevant literature was identified using databases including Scopus, Web of Science, IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar. The search employed keywords such as Artificial Intelligence, Credit Card Fraud Detection, Machine Learning, Deep Learning, Predictive Analytics, Anomaly Detection, and Digital Payments.

Selection Criteria

The review primarily includes studies published between 2018 and 2024. Only English-language, peer-reviewed publications and credible industry reports directly related to AI-based credit card fraud detection were considered. Duplicate, outdated, and irrelevant studies were excluded.

Data Analysis

The selected literature was examined using thematic analysis. The studies were grouped into key themes, including AI techniques, fraud detection methods, benefits, implementation challenges, ethical concerns, and future research directions. The findings were critically reviewed and synthesized to present a comprehensive overview of AI-driven credit card fraud detection.

FINDINGS

The review reveals that Artificial Intelligence (AI) has significantly transformed credit card fraud detection by enabling faster, more accurate, and adaptive identification of fraudulent transactions. Machine learning, deep learning, predictive analytics, and anomaly detection are the most widely adopted AI techniques for detecting evolving fraud patterns in real time. The literature consistently indicates that AI-driven systems outperform traditional rule-based approaches by reducing false-positive alerts, improving detection accuracy, and supporting real-time transaction monitoring. These capabilities strengthen fraud prevention while enhancing operational efficiency and customer trust in digital payment systems. The review also identifies key challenges associated with AI adoption, including data privacy, algorithm transparency, regulatory compliance, implementation costs, and cyber security risks. Addressing these challenges is essential to ensure the effective and ethical deployment of AI in the banking sector. Overall, the reviewed studies highlight that AI has become a strategic tool for strengthening financial security and combating increasingly sophisticated credit card fraud. Continued technological advancement, responsible AI governance, and collaboration among banks, fintech firms, and regulators will be critical to enhancing the resilience of digital payment ecosystems.

IMPLICATIONS OF THE STUDY

This review highlights the growing role of Artificial Intelligence in strengthening credit card fraud detection through improved accuracy, real-time monitoring, and proactive risk management. The findings provide useful insights for banks and fintech firms to enhance fraud prevention strategies, while supporting policymakers in developing secure and ethical AI governance frameworks. The study also serves as a reference for researchers by consolidating current knowledge and identifying emerging areas in AI-enabled financial security.

FUTURE RESEARCH DIRECTIONS

Future research should explore emerging technologies such as Explainable AI (XAI), Generative AI, and block chain-based fraud detection to improve transparency, security, and decision-making. Comparative studies across countries and longitudinal research on AI adoption will further strengthen understanding of its effectiveness in combating evolving credit card fraud.

CONCLUSION

Artificial Intelligence has emerged as a transformative technology in credit card fraud detection by enabling faster, smarter, and more accurate identification of fraudulent transactions. The reviewed literature indicates that

AI-driven techniques outperform traditional rule-based systems by improving detection efficiency, reducing false positives, and enhancing financial security. Despite challenges related to data privacy, transparency, and regulatory compliance, AI continues to play a pivotal role in strengthening digital payment ecosystems. As financial fraud becomes increasingly sophisticated, sustained innovation, responsible AI implementation, and collaborative regulatory efforts will be essential for building secure and resilient banking systems.

REFERENCES:

- 1) Aggarwal, C. C. (2015). *Data mining: The textbook*. Springer.
- 2) Bahnsen, A. C., Aouada, D., Ottersten, B., & Stojanovic, A. (2016). Feature engineering strategies for credit card fraud detection. *Expert Systems with Applications*, 51, 134–142. <https://doi.org/10.1016/j.eswa.2015.12.030>
- 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. <https://doi.org/10.1016/j.dss.2010.08.008>
- 4) Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical Science*, 17(3), 235–255. <https://doi.org/10.1214/ss/1042727940>
- 5) 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. <https://doi.org/10.1016/j.inffus.2017.09.005>
- 6) Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, 41(3), 1–58. <https://doi.org/10.1145/1541880.1541882>
- 7) Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.
- 8) IBM Corporation. (2024). *Cost of a data breach report 2024*. IBM Security.
- 9) Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P. E., He-Guelton, L., & Caelen, O. (2018). Sequence classification for credit-card fraud detection. *Expert Systems with Applications*, 100, 234–245. <https://doi.org/10.1016/j.eswa.2018.01.037>
- 10) LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436–444. <https://doi.org/10.1038/nature14539>
- 11) 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. <https://doi.org/10.1016/j.dss.2010.08.006>
- 12) Reserve Bank of India. (2024). *Report on trend and progress of banking in India 2023–24*. Reserve Bank of India.
- 13) Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.
- 14) Schmidhuber, J. (2015). Deep learning in neural networks: An overview. *Neural Networks*, 61, 85–117. <https://doi.org/10.1016/j.neunet.2014.09.003>
- 15) Visa Inc. (2024). *Visa payment fraud disruption report*. Visa.
- 16) World Economic Forum. (2024). *Global cybersecurity outlook 2024*. World Economic Forum.
- 17) World Bank. (2024). *World development report 2024: Digital transformation*. World Bank.
- 18) Zou, J., & Schiebinger, L. (2018). AI can be sexist and racist—It's time to make it fair. *Nature*, 559(7714), 324–326. <https://doi.org/10.1038/d41586-018-05707-8>
- 19) European Union Agency for Cybersecurity (ENISA). (2023). *ENISA threat landscape 2023*. ENISA.
- 20) Financial Stability Board. (2024). *The financial stability implications of Artificial Intelligence*. Financial Stability Board.
- 21) Hand, D. J., & Whitrow, C. (2008). Statistical techniques for fraud detection. *Encyclopedia of Quantitative Risk Analysis and Assessment*. Wiley.
- 22) He, H., & Garcia, E. A. (2009). Learning from imbalanced data. *IEEE Transactions on Knowledge and Data Engineering*, 21(9), 1263–1284. <https://doi.org/10.1109/TKDE.2008.239>
- 23) Kou, Y., Lu, C. T., Sirwongwattana, S., & Huang, Y. P. (2004). Survey of fraud detection techniques. *IEEE International Conference on Networking, Sensing and Control*, 749–754.
- 24) Mastercard. (2024). *Cyber security and digital payments report*. Mastercard.
- 25) National Payments Corporation of India. (2024). *Annual report 2023–24*. NPCI.