I J C R M
International Journal of Contemporary Research In Multidisciplinary

Research Article

Integration Challenges and Success Factors for AI-based Fraud Prevention in Indian Banking: A Legal and Constitutional Perspective

Lokendra Patel [1*], Dr. Priyanka Gupta [2]
[1] Research Scholar, NIMS University, Jaipur, Rajasthan, India
[2] Associate Professor, NIMS University, Jaipur, Rajasthan, India

Corresponding Author: *Lokendra Patel

DOI: https://doi.org/10.5281/zenodo.20153422

Abstract

The study investigates the correlation between legal and regulatory clarity and the efficient implementation of AI-based fraud prevention systems in Indian banks, and how data privacy and constitutional rights, including the right to privacy under Article 21, influence their design and deployment. Using the qualitative approach, the study provides an analysis of secondary resources such as scholarly literature, legal documents, and policy reports to assess the operational, legal, and moral problems of the use of AI. The results prove that AI has great potential but can be effective in reducing fraud only due to fragmented legal frameworks, poor transparency of the algorithms used and data privacy and due process issues under the constitution. The lack of regulations specific to AI results in inconsistency in operation, but doctrines provided under the existing laws, such as the DPDP Act and judicial precedents, provide partial guidance. This study recommends that a unified rights-aware regulatory regime would be critical in sound and responsible integration of AI in the domain of fraud prevention, which would eliminate the issue of technological progress overcoming the law and the limits imposed by ethics.

Manuscript Information

- **ISSN No:** 2583-7397
- **Received:** 01-04-2026
- **Accepted:** 15-04-2026
- **Published:** 13-05-2026
- **IJCRM:**5(3); 2026: 136-142

- **Plagiarism Checked:** Yes
- **Peer Review Process:** Yes

How to Cite this Article

Patel L, Gupta P. Integration Challenges and Success Factors for AI-based Fraud Prevention in Indian Banking: A Legal and Constitutional Perspective. Int J Contemp Res Multidiscip. 2026;5(3): 136-142.

Access this Article Online

www.multiarticlesjournal.com

KEYWORDS: AI-based fraud detection, Indian banking, legal framework, data privacy, constitutional rights, regulatory challenges, algorithmic transparency, digital security, Article 21.

1. INTRODUCTION

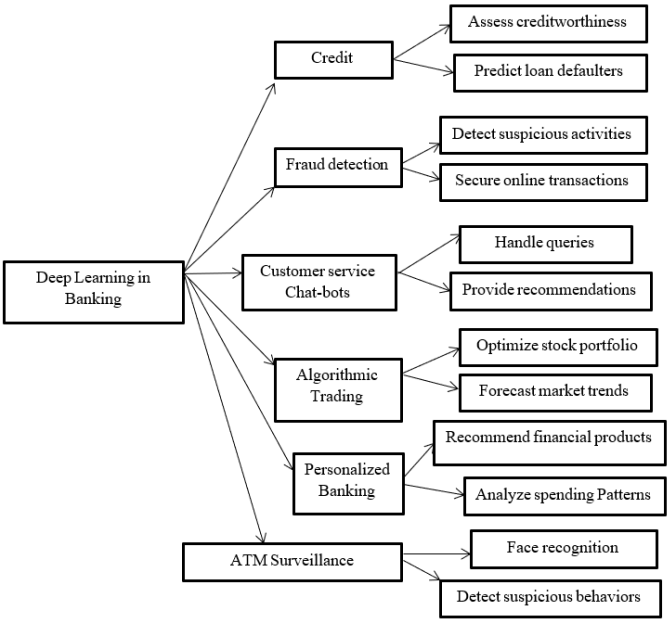
The deployment of AI-driven fraud detection systems in Indian banking involves a complicated interaction between technological potential and legal-constitutional examination. On one hand, AI is indispensable in achieving significant success factors such as improved real-time monitoring, predictive analytics, and anomaly detection that can greatly diminish the risks of financial fraud (Olufemi et al 2024). Nonetheless, the implementation of AI is faced with challenges like the privacy of data, the bias of the algorithm, the lack of a regulatory framework that is open and constructive, and the limited capacity of both public and private banks (Goyal 2024). From a legal perspective, AI usage is obligated to adhere to legal procedures like due process, proportionality, and non-arbitrariness that are guaranteed in the Indian Constitution, particularly under Articles 14 and 21.

Moreover, in the absence of a data protection law that is all-inclusive, the legal processing of customer data by AI systems becomes a matter of concern. A practical approach to ensure proper execution is required, one that can offer the right room for innovation as well as the integration of strong legal safeguards, an accountable institution, and an operative regulatory framework parallel to the constitutional mandates (Menon 2022). The current digital era has facilitated the rise of online transactions, e-commerce, and digital banking, hence providing new avenues for fraudsters to exploit weaknesses in financial systems. Cybercrime is escalating, with increasingly complex schemes that target individuals, corporations, and governments. These schemes encompass phishing assaults, identity theft, and more intricate kinds of financial crime, including account takeovers and money laundering (Ratan 2025). The swift advancement of these fraudulent operations presents considerable hurdles for conventional fraud detection and prevention techniques, which frequently fail to match the speed and creativity of contemporary cybercriminals.

Robust fraud prevention measures are essential for defending financial institutions, preserving customer trust, and assuring the stability of economic operations. The financial repercussions of fraud may be catastrophic for both individuals and organisations, resulting in considerable economic consequences and reputational harm (Joshi 2024). Furthermore, regulatory authorities are placing greater emphasis on the necessity for effective fraud prevention systems to adhere to rigorous legal standards. Implementing effective fraud protection techniques mitigates financial losses and enhances the resilience of financial institutions against prospective assaults. It guarantees a safe digital environment, cultivating trust and confidence among consumers and stakeholders (Kumar 2024).

"The right to privacy is inextricably bound up with all exercises of human liberty – both as it is specifically enumerated across Part III, and as it is guaranteed in the residue under Article 21. It is distributed across the various articles in Part III and, mutatis mutandis, takes the form of whichever of their enjoyment its violation curtails"

The emergence of technology has significantly transformed the banking sector. Digital banking, a component of the expansive financial technology (FinTech) sector, pertains to the use of electronic platforms for executing banking transactions. This may encompass online banking platforms and mobile applications (Kinetics 2025). These digital platforms enable users to execute a multitude of operations, ranging from verifying account balances to facilitating international financial transfers, all conveniently accessible. Furthermore, the emergence of blockchain technology and cryptocurrencies has added a novel aspect to the banking sector, contesting conventional concepts of money and transaction processing (CXOtoday News Desk 2025). Considering the pivotal function of banks in the economy, a comprehensive regulatory framework is vital to maintaining their stability and integrity. Regulatory authorities, often at the national level, establish norms and criteria that banks are required to follow. These rules encompass a broad range of domains, from capital adequacy standards to consumer protection provisions (Findoc 2025). Following financial crises, these policies are often reassessed and amended to mitigate systemic risks.



Source: https://core.ac.uk/download/pdf/578755756.pdf

Figure 1: Deep learning in modern banking and finance

AI-based fraud detection in banks across India is the approach that needs unique success conditions and is subject to serious legal and constitutional dilemmas. The regulatory framework in India is disparate and comprises the Reserve Bank of India (RBI), Digital Personal Data Protection Act (DPDPA) 2023, and historical legislation such as the Information Technology Act 2000 and Banking Regulation Act 1949, which make up an incomplete jigsaw puzzle of controlling AI systems (Ani 2025). Such a regulatory vacuum leaves major holes in liability models of AI systems, making incorrect decisions against such rules as the denial of a wrongful transaction or the inability to notice a fraud time when long-established principles of human agency and foreseeability found in traditional legal systems do not easily translate to intelligent algorithms (Victoria 2025). Cases of algorithmic bias in fraud detection raise constitutional

concerns both because they may discriminate against previously discriminated groups based on false positives (undermining the right to equality in Article 14), and because closed-source black box" systems perform this kind of bias in a way that cannot be effectively challenged under Article 21, undermining the right to due process (JusCorpus 2025).

Another form of conflict between the constitutional provisions is data privacy, because fraud prevention using AI necessitates huge data processing contradictory to the fundamental right to privacy in *Justice K.S. Puttaswamy v. United States of India*. The DPDP Act 2023 has not adequately regarded AI-specific data use in terms of the limitation to purpose with transparency in the algorithms. There is also a problem of infrastructural barriers: poor digital literacy (only 20 per cent of Indian adults are digitally literate) hinders the effectiveness of the systems, and weaker data quality in various institutions presents unreliability when assembling a dataset to train AI. The changing strategies of fraudsters require frequent updates of the models, and most of the banks do not have sufficient resources to provide them (Ani 2024). The implementation process has to take care of technological as well as constitutional imperatives to be successful.

Legal, technical, and ethical cross-functional teams should come up with AI systems that have in-built constitutional safeguards such as frequent bias auditing and impact assessment in line with fundamental rights (Cio, E. 2024). AI frameworks are needed not only for technical, transparent reasons but also as a requirement of due process, so that customers can see and challenge the adverse determinations made. Advantages consist of training programs of the staff as prescribed by the Department of Financial Services to strengthen the possibilities of human control, and multi-level security based on the combination of AI, behavioural biometrics, and risk-based authentication, mitigating the use of algorithms (Jadhao 2025).

The study aims to examine the integration challenges and success factors of AI-based fraud prevention in Indian banking, with a focus on the legal and constitutional frameworks governing data privacy, regulatory compliance, and fundamental rights.

The paper is structured into eight sections. Section 1 comprises the introduction of the document. Section 2 presents a literature evaluation of the cases and previous research. Section 3 delineates the goals. Section 4 addresses the hypothesis. Section 5 delineates the research technique. Section 6 resulted in an output aligned with the goals. Section 7 continues with the discourse. Section 8 includes findings, consequences, limits, and suggestions for further study. References have been integrated.

2. LITERATURE REVIEW

Following a systematic literature review, it became evident that numerous studies had been conducted to explore the potential of AI in the banking and financial industries and its impact on the sectors' transformative changes. Particularly, it was so within the areas of fraud detection, risk management, and digital transformation. Kumar et al. (2024) clearly brought out the rapid progress of AI in the Indian banking system in their article by highlighting automation, customer experience, regulatory compliance, fraud detection, and prudent risk management. In their research, they reported examples of AI-based chatbots in the State Bank of India, with which they mentioned offsetting factors like data privacy, legal compliance, and job displacement.

As a support, Ridzuan et al. (2024) offered a detailed account of the applications, benefits, and challenges of AI, while discussing the ethical and legal aspects of AI in the context of world markets, such as the rules and frameworks for the governance of ASEAN and AI. The authors went further in proposing that the blending of UTAUT and institutional theory could help in shaping recommendations for future research. The study by Aziz and Andriansyah (2023) targeted the field of AI-assisted fraud prevention, which was addressed through examples of deep learning models, neural networks, NLP-enhanced KYC, graph analytics, and behaviour biometrics. The text emphasised the elasticity of AI and how it was applied to fight against financial predations. On the same note, Maharana (2025) researchers went into further discussion about the dual role, consisting of prevention and allowance of financial fraud in India, usage of AI in phishing and impersonation attacks by cybercriminals, as well as an investigation of the role of AI in identifying anomalies.

In addition, Shan (2025) examined the risk of fraud enabled by AI and the response to it, including LLMs, liveness testing, and machine learning-based detection, and suggested adaptive responses to new threats. Discussed legal aspects, the study by Chatterjee and NS (2022) related to the impact of AI on human rights, civil/criminal liability, examined the Indian and international legal system and proposed its regulation to the changes in a fast-growing technology. Chintala and Yamijala (2023) provided a sharp case study of the Bank of Maharashtra and highlighted the importance of AI in risk regulation as well as screening of fraud and ethical governance, encouraging a balanced implementation approach. Prakash and Deokar (2025) discussed the importance of explainable AI in establishing transparency in determining fraud involving the monitoring of transactions and identity confirmation, and encouraged the ongoing innovations to keep foul play at bay.

Yekollu et al. (2024) emphasised the importance of real-time adaptability and effective data governance in the context of AI-based fraud detection systems, highlighting the constraints of deep learning models associated with scalability and explainability. In the situation of the COVID-19 pandemic, Sinha et al. (2022) examined how AI could fight digital fraud, including phishing and malware, as well as the wider implications of AI on the responsiveness and satisfaction with businesses. Rawal et al. (2025) expressed concern with the capabilities of generative AI and prevention of fraud and addressed its future potential in the protection of financial institutions, including the ethical issues of its usage. The study by Pahari et al. (2023) focused on the adoption of AI by Indian private banks, mentioning optimisation cost-cutting, operation optimisation, and increasing revenue growth as its benefits, and determined the hindrance to AI maturity.

The study by Dash et al. (2023) compared traditional machine learning methods and new neural networks and identified better

results in detecting fraud using AI models, emphasising the importance of quality and management of data. Al-Fatlawi et al. (2024) suggested a genetic algorithm-based fraud detection model based on the AI approach and compared it with the decision and regression trees method to prove its capability to prevail over other approaches in detecting intrusions in electronic banking. Pillai and Latha (2025) addressed the increasingly popular cyberbanking fraud issue and explained why real-time detection systems based on AI and ML were the way to go when it came to maintaining consumer confidence. Finally, Zainal (2023) summarised the use of AI and Big Data in detecting anomalies, referencing the possibility of combining machine learning and behavioural analysis to predict fraud, as well as the limitations formed by scalability, bias, and data privacy issues.

3. OBJECTIVE

- To examine the relationship between legal and regulatory clarity and the effective implementation of AI-based fraud prevention systems in Indian banks.
- To analyse how data privacy and constitutional rights (such as the right to privacy under Article 21) influence the design and deployment of AI-driven fraud detection systems in Indian banks.

4. Hypothesis

H1: There is a significant positive relationship between the clarity of legal and regulatory frameworks and the successful implementation of AI-based fraud prevention technologies in Indian banking.

H2: Constitutional concerns related to privacy significantly influence the design, deployment, and operational scope of AI-based fraud prevention tools in Indian banking institutions.

5. RESEARCH METHODOLOGY

This study utilises a qualitative research approach, using both descriptive and explanatory research methodologies to thoroughly investigate and analyze the topic. The study predominantly utilises secondary data sources, such as academic literature, policy papers, government reports, and pertinent publications, to evaluate available material and derive significant findings.

6. RESULT

Objective 1: To examine the relationship between legal and regulatory clarity and the effective implementation of AI-based fraud prevention systems in Indian banks**.**

In Indian banks, the availability of legal and regulatory mandates supports the system of implementing AI-based fraud prevention systems. Lack of AI regulations specific to India, in the form of algorithmic bias and false positives, inconsistency in risk management and exposure to cybersecurity vulnerabilities, are the current factors that challenge the operational capacity of current AI-based fraud systems (S.S. Rana 2025). Established legal frameworks already offer some sources of foundations, and yet they are not AI-specific, including the Prevention of Money Laundering Act (2002) and Digital Personal Data Protection Act (2023), which can provide the basis in data governance; however, these do not include the aspect of algorithmic transparency or mitigation of bias. Regulatory transparency increases the degree of trust and effectiveness of systems, and data indicate that simpler structures work to improve results directly (Rai 2025). As an example, standardised fraud AI can secure $9 billion in annual cost savings by the year 2025. EU AI Act and the U.S. SEC guidelines are prime examples of global precedent, which show that risk-classification frameworks can minimise false positives by 30% and limit algorithm biases by 22% (Das 2024). Clarity in regulating AI is vital in enhancing fraud avoidance in AI. The use of tools such as Mulehunter.ai and surveillance by SEBI reveals the promise of progress in India, and generalised AI-specific rules will be necessary in providing a uniform and ethically sound implementation of AI within the banking industry (Kumar 2024). Otherwise, there will be systemic risks and unbalanced adoption. The legal and regulatory certainty serves as a driver as well as a regulator towards the efficacy of the application of AI-based fraud prevention systems in Indian banks. Although such step-by-step regulations and enactment of Acts such as the DPDP have been significant in India, there is a lack of a unified framework of AI, which brings in the element of uncertainty (vajiramandravi 2025). This will require a balanced, rights-conscious, and innovation-friendly regulatory environment that will fulfil the potential of AI to safeguard a banking ecosystem against complex threats of fraudulent activities (Yadav 2024).

Table 1: Current Regulatory Landscape in India

Legal/Regulatory Tool	Relevance to AI-based Fraud Detection
DPDP Act, 2023	Regulates consent-based data processing; crucial for AI model training.
RBI Master Directions on Digital Payment Security Controls (2021)	Mandates fraud risk management and supports the use of automated tools.
RBI's Framework for Regulatory Sandbox (2019)	Encourages experimentation with AI tools under regulatory supervision.
IT Act, 2000 (amended)	Covers cybercrime and digital evidence, providing a legal backdrop for AI-based fraud detection.
SEBI and IRDAI Guidelines (for related financial entities)	Influence risk-based AI implementation in adjacent sectors like insurance and securities.

Objective 2: To analyse how data privacy and constitutional rights (such as the right to privacy under Article 21) influence the design and deployment of AI-driven fraud detection systems in Indian banks.

The establishment and implementation of the AI-based fraud detection system in the Indian banks is significantly supported by the right of privacy in the Indian Constitution mentioned in Article 21 and the evolving data protection standard. The conjunction of technological advancement and constitutionalism, as well as legal rights, produces additional potentials and limitations to the Indian financial institutions implementing AI in the fight against fraud. The verdict of the Supreme Court on the case judgment of Justice K.S. Puttaswamy and another v. Union of India (2017) considered the right to privacy as it reflects the right to informational privacy and autonomy over personal data regarding Article 21

as a fundamental right. This move established a three-fold test of any impairment of the right to privacy, which includes legitimacy, necessity and proportionality (Yadav 2025). Banks should have AI systems that are legally grounded, limited in their purpose, and minimally invasive. Digital Personal Data Protection (DPDP) Act, 2023 gives a system to data privacy which involves information that needs permission, and it should be utilised lawfully; information minimisation and limitation of storage; and data subject rights (Ani 2025). These rights influence the design of the AI systems, especially in the expandability of the AI decisions, and the human-in-the-loop mechanism of appeals or mending incorrect fraud flags. AI systems in banking have design implications, which include legal/constitutional issues, design/operational influence on AI systems, as well as security and privacy (Signzian 2024). The examples of AI-based systems are the SAS Fraud Framework deployed by Private sector banks such as HDFC and ICICI, and the Yono layers deployed by the State Bank of India (SBI) to detect fraud. The AI engine of Unified Payments Interface (UPI), Pai.AI, detects suspicious transactions done in Google Pay and PhonePe, demanding a high level of privacy standards. Regulatory issues involve proportionality surveillance, the responsibility of RBI in regard to cybersecurity and guidelines to deal with fraud, as well as specific industry privacy advice with respect to constitutional jurisprudence (Gouda 2024). Privacy by Design (PbD), Impact Assessments, Human Oversight, and Audit Trails, as well as Inter-agency Harmonisation, are some of the propositions of rights-fitted AI implementation. The development of AI-based fraud detection in the Indian banking context should be anchored in the system of rights-based boundaries, the pillar of which is Article 21 of the Constitution and a set of legal provisions contained in the DPDP Act, 2023. Dual imperatives of personal choice and financial security are to be ensured by adherence to meticulous legal constraints, effective technical protection, and transparent and accountable AI governance. Uncertainty about the trustworthiness of AI systems in the context of banking extends beyond the question of their accuracy and applies to their constitutional and ethical legitimacy too (Academike 2024).

7. DISCUSSION

The research presents an influential combination of theoretical knowledge and empirical recommendations about AI in the Indian banking industry. The authors, among whom are Kumar et al. (2024), Ridzuan et al. (2024), Aziz and Andriansyah (2023), Maharana (2025) and others, focus on the transformative role of AI in terms of fraud detection and risk management, as well as customer engagement. Kumar et al. (2024) emphasise the use of AI, such as chatbots, and the ethics concerning data privacy and compliance, whereas Rizuan et al. (2024) put ethical issues of AI into the framework of global governance. In the meantime, Aziz and Andriansyah (2023) point out deep learning, KYC optimisation, and behavioural biometrics in counter-fraud applications. A technical-legal interface is covered by Shan (2025) and Chatterjee & NS (2022) in the form of artificial intelligence as an alternative and a menace, primarily in the form of algorithmic choices that may restrain constitutional safeguards, including the right to individual liberty from arrest under Article 21. All these academic arguments are in line with the findings section, where it becomes evident that, notwithstanding the backing provided by available frameworks such as the DPDP Act 2023 or the instructions that the sandbox offers in the RBI, Indian banks are hampered by the lack of coherent regulation, the absence of clarity as to any AI legal implications, and consistent algorithmic accountability (S.S. Rana 2025; Rai 2025). The study demonstrates that legal certainty leads to a higher rate of implementation success, and those international practices, such as the EU AI Act and the SEC regulations in the U.S., are favourable ones to emulate. Such regulatory clarity has been touted as both economically and security beneficial by authors such as Das (2024) and Kumar (2024). Moreover, *Justice K.S. Puttaswamy v. Union of India* Technological implementation of AI tools is placed within the existence of legitimate, necessary and proportionate grounds of the rule of law of binding applications in the Union of India and the three-prong test. Other operational AI tools of the form Yono utilised by SBI, UPI included, mentioned by the study should comply with the norms of technical efficiency as well as data rights.

8. CONCLUSION

In conclusion, the AI-based fraud prevention systems incorporated into Indian banking demonstrate a complicated but necessary interplay of technological development, the justice system, and the constitutional protection. Although being the most powerful tool in terms of crime detection (fraud, in particular), surveillance of financial activity, and risk mitigation, AI implementation is impaired by incoherent regulatory frameworks, the absence of algorithmic visibility, and issues emerging regarding data protection and human rights in general. The legal framework regarding AI is not present at all in India, and, as a result, banks are not able to implement any AI tools that would be simultaneously effective and not contravening the Constitution. In addition, issues like biased algorithms, infrastructure deficiency, and digital illiteracy also restrict the just and efficient implementation of such technologies. However, current legal provisions are giving rise to some pillars on which future AI systems should be implemented, such as the law on the protection of data and the acceptance of the right to privacy by the courts. The key to effective utilisation of these tools is the golden mean- creating conditions under which technological innovation is entrenched with checks and balances such as human control, transparency and proportionality to fulfill the constitutional provisions. A unified regulatory regime, a combination of rights-based AI development, as well as a great institutionalising accountability will play a decisive role in creating a trusted yet resilient banking eco-system, which will combat fraudulent threats reaching higher levels.

REFERENCES

1. Academike. Safeguarding personal privacy in the era of artificial intelligence systems. 2024 Oct 14.
2. Al-Fatlawi A, Talib Al-Khazaali AA, Hasan SH. AI-based model for fraud detection in bank systems. Fusion Pract Appl. 2024;14(1).

3. ANI. Banks to use AI & machine learning to safeguard customers from financial fraud. The Economic Times. 2024.
4. ANI. Indian banks must urgently embrace AI, privacy technologies to comply with DPDP Act: Report. The Economic Times. 2025 Jun 9.
5. Aziz LAR, Andriansyah Y. The role of artificial intelligence in modern banking: AI-driven approaches for fraud prevention, risk management, and regulatory compliance. Rev Contemp Bus Anal. 2023;6(1):110–132.
6. Chatterjee S, NS S. Artificial intelligence and human rights: Indian legal and policy perspective. Int J Law Manag. 2022;64(1):110–134.
7. Chintala PRS, Yamijala LSB. AI for fraud prevention in banking: Challenges and opportunities. 2023.
8. Cio E. Banks to use AI & machine learning to safeguard customers from financial frauds. ETCIO. 2024 Dec 7.
9. Constitution of India. Article 14. 1950.
10. Constitution of India. Article 21. 1950.
11. CXOToday News Desk. AI, fraud prevention & digital spend: How Indian banks are reinventing themselves. 2025 Jun 17.
12. Dalvi A. Banking AI: 7 real challenges with actionable fixes. 2025 Apr 30.
13. Das N. RBI policy acts big on banking frauds: MuleHunter.ai tool. The Economic Times. 2024 Dec 12.
14. Dash S, Das S, Sivasubramanian S, Sundaram NK, KG H, Sathish T. Developing AI-based fraud detection systems for banking and finance. In: Proc ICIRCA; 2023 Aug. p. 891–897.
15. Digital Personal Data Protection Act (DPDPA). 2023.
16. Economic Survey. Indian banks bet big on AI, but "black-box" risks loom. Moneycontrol. 2025 Jan 31.
17. Feedzai. AI fraud trends 2025: Banks fight back. 2025 May 6.
18. Findoc. AI vs banking fraud: How Indian banks are getting smarter. 2025 Jun 22.
19. Flinders M, Smalley I, Schneider J. AI fraud detection in banking. 2025 Apr 30.
20. Gouda S. Navigating the ethical landscape: Right to privacy in the age of AI. Int J Res Innov Soc Sci. 2024;8(8):128–137.
21. Goyal D, Monga D. Role of AI in combating corporate fraud in financial sectors. Int J Res Publ Rev. 2024;5(11):1877–1885.
22. Jadhao PA. Legal implications of AI in the Indian banking sector. Int J Res Publ Rev. 2025;6(5):2834–2836.
23. Joshi A. Artificial intelligence and machine learning in banking: A legal perspective. 2024 Jul 15.
24. JusCorpus. Legal challenges of deepfake technology in India. 2025 Apr 20.
25. Justice KS Puttaswamy v. Union of India. 2017.
26. Cloud Kinetics. How banks fight fraud with AI analytics. 2025 Feb 17.
27. Kumar D. Responsible AI in finance: RBI perspective. 2024 Dec 21.
28. Kumar K, Kuhar N, Sharma M. Artificial intelligence in the Indian banking system: A systematic review. Proc ICOFE. 2024.
29. Maharana N, Kuppili SK, Ganesh BUB, Das GP, Chaudhury SK. Financial fraud in India in the age of AI. IGI Global. 2025:317–340.
30. Menon B, Nooshian K. Application of AI in fraud detection in banking industry. 2022.
31. Olufemi B, Bello O, Komolafe O. Artificial intelligence in fraud prevention. 2024;5:1505–1520.
32. Pahari S, Polisetty A, Sharma S, Jha R, Chakraborty D. Adoption of AI in Indian banking. Indian J Mark. 2023;53(3):26–41.
33. Pillai RP, Latha DPP. AI in banking sector for fraud detection. IGI Global. 2025:359–382.
34. Prakash V, Deokar R. Harnessing AI for fraud detection in banking. 2025:389–406.
35. Rai P, Shekhar C. AI in financial markets: Regulatory challenges. Int J Res Publ Rev. 2025;6(3):5503–5516.
36. RaptorX. Navigating financial crime in Indian banking. 2025.
37. Ratan A, Ciso E. AI vs AI in banking fraud detection. ETCISO. 2025 May 24.
38. Rawal R, Sachdeva P, Singhvi AS. Generative AI in fraud detection in banking. 2025:159–173.
39. Ridzuan NN, Masri M, Anshari M, Fitriyani NL, Syafrudin M. AI in financial sector: Innovation and ethics. Information. 2024;15(8):432.
40. S.S. Rana & Co. AI in finance sector: Ethics & law. 2025 May 16.
41. Saravanan G. AI-powered fraud detection in finance. 2025 Jun 3.
42. Shan W. AI-powered fraud detection in banking (Doctoral dissertation). 2025.
43. Signzy. Supreme Court judgement & re-birth of privacy. 2024 Jul 22.
44. Sinha M, Chacko E, Makhija P. AI technologies for banking fraud during COVID-19. Springer. 2022:443–459.
45. Vajiram & Ravi. RBI panel for ethical AI adoption. 2025 May 6.
46. Victoria A. AI-driven fraud detection and financial inclusion in India. 2025 May 19.
47. Yadav J, Giri A. Privacy in the age of artificial intelligence. Int J Creat Res Thoughts. 2025;13(3):980–981.

48. Yadav P. RBI to launch AI system for fraud alerts. Inc42. 2024 Oct 29.
49. Yekollu RK, Haldikar SV, Ghuge TB, Farook O, Biradar SS. AI-powered fraud detection in banking transactions. In: Proc IEEE CICN; 2024 Dec. p. 559–564.
50. Zainal A. Role of AI and big data in fraud prevention. Int J Adv Cybersecurity Syst Technol Appl. 2023;7(12):1–10.

About the Corresponding Author

Lokendra Patel is a Research Scholar at NIMS University, Jaipur, Rajasthan, India. His academic interests focus on emerging technologies, particularly artificial intelligence and its applications in banking, finance, and legal frameworks. He is actively engaged in research addressing fraud detection, data privacy, and regulatory challenges in the digital financial ecosystem.