IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AI-INDUCED RISKS IN INDIA'S FINTECH SECTOR: AN EVALUATION OF RBI'S REGULATORY RESPONSE

[1]Soumya Ranjan Nayak

[1]Assistant Professor,
[1]Department of Economics,
[1]Govt. B.Ed. Training College Kalinga, Kandhamal, India

Abstract: The rapid integration of Artificial Intelligence (AI) and Machine Learning (ML) has introduced vulnerabilities within India's FinTech sector. These vulnerabilities are mainly adversarial attacks, deepfake fraud, and algorithmic bias. This current study has done a qualitative document analysis to evaluate the alignment of AI risks affecting the fintech sector and the regulatory framework of the Reserve Bank of India (RBI). The study has found that the RBI has a robust governance layer. The RBI requires banks to use outsourced services with strict liability, consumer consent, and full accountability. However, this study has found that RBI policies have largely failed to implement specific technical and model-level safeguards. For core practices like mandatory algorithmic fairness audits, model robustness testing, and specific methodologies for explainability, there is no binding requirement in RBI's regulatory framework. The study finally concludes that RBI has existing strong governance principles. Therefore, RBI's framework must evolve to integrate granular technical standards. This creates a safeguard for the digital financial ecosystem against complicated threats of modern AI and Generative AI systems**.**

***Index Terms* -** RBI Regulation, FinTech Risk, AI Governance, Algorithmic Bias, Generative AI.

I. INTRODUCTION

Artificial Intelligence (AI) and Machine Learning (ML) have become central to the functioning of modern financial services, especially within digitally driven fintech ecosystems. These technologies are used for many banking related activities like credit scoring, fraud detection, onboarding processes, behavioural profiling, and customer engagement. Due to use of these technologies' new vulnerabilities such as model instability, adversarial manipulation, algorithmic unfairness, and data-governance challenges arise (Feyen et al., 2021). These days Generative AI has further expanded this risk landscape. Its products like deepfake-based identity fraud, synthetic data manipulation, and sophisticated social-engineering attacks threaten both consumer safety and institutional resilience (FSB, 2024).

India's fintech sector, characterised by rapid adoption of digital lending, biometric verification, algorithmic credit assessment, and API-driven service delivery, increasingly depends on these AI systems. Correspondingly, the Reserve Bank of India (RBI) has developed several regulatory instruments addressing digital finance, cybersecurity, consumer protection, outsourcing, and model governance. But as fintech becomes more AI-dependent the polity perspective must be reviewed. Biggest question is what the extent to which these regulatory frameworks address contemporary AI-enabled risks.

This study examines the alignment between AI-induced risks in fintech and RBI's current regulatory architecture. This study mainly focusses on consumer-facing and institution-facing vulnerabilities. Key RBI regulations alongside documented AI threats will be analyzed then structured assessment of regulatory coverage will be done in this paper. This is important as India transitions toward a more AI-intensive financial environment.

2.Literature Review

2.1 AI-Induced Risks in FinTech

Today fintech ecosystem faces new type of threats due on-going developments in AI technologies. (Saha et al., 2025) has classified AI-related threats into two broad categories: (a) threats enabled by Generative AI and (b) threats targeting AI systems themselves. These threats are either complex attacks on AI models or malicious use of AI tools for financial related fraud.

AI systems themselves are increasingly vulnerable to adversarial manipulation. (Kumar, 2024) notes that AI models can be deceived by attackers through techniques such as prompt injection, which enables malicious actors to override security safeguards in LLM-based chatbots (Digital Thread Report 2024; Saha et al., 2025) provide a detailed examination of technical attacks such as model inversion, data poisoning, adversarial inputs, and model theft, all of which can compromise AI models deployed by financial institutions.

The complexity of modern AI systems increases AI induced risks. Many AI/ML models operate as black boxes. Black boxes limit transparency and explainability for stakeholders like analysts, auditors, and regulators. The blind spots undermine trust and complicate compliance efforts (Kumar, 2024). A study by (Vučinić & Luburić, 2024) highlights when AI systems gain greater autonomy in decision-making, there is rise in operational and reputational risks. Another risk is AI systems depend heavily on large volumes of sensitive consumer data which raising serious privacy and ethical concerns (Kumar, 2024).

Algorithmic bias is another important type of danger that comes up. AI and ML algorithms may unintentionally reinforce historical and cultural prejudices which can lead to biased results in lending, credit scoring, and fraud detection. Algorithmic bias can result in result in “vicious cycle of financial exclusion” for certain consumer groups. (Fintech Lending Risk Barometer 2024) and (Kagalwala et al., 2024) . This bias can also lead to ethical and societal risks like displacement of human labour and the propagation of misinformation. (Saha et al., 2025).

AI-driven fraud and deception are becoming complex day by day. The (FinSec: An Emerging Equation between FinTech and Cybersecurity, 2025) report notes the growing use of deepfakes to create synthetic identities capable of bypassing KYC and AML systems. AI is used by scammers to design personalised attack targeted towards consumers (Saha et al., 2025). By using malicious Generative AI models such as WormGPT and FraudGPT low-skilled scammers are able to launch complex cyber attacks on consumers and institutions. (Digital Thread Report 2024, 2024; Saha et al., 2025). Misinformation and disinformation manufactured and spread with the help of AI for market manipulation and other financial disruption. (Artificial Intelligence in Financial Services, 2025)

2.2 RBI Regulations on AI

Several studies have examined the Reserve Bank of India's regulatory measures concerning fintech, which indirectly address AI dangers. (Saha et al., 2025) analysed the efforts of RBI’s Framework for Responsible and Ethical AI (FREE-AI) Committee in some detail. These RBI reports suggest guidelines for the use of AI in financial services. The RBI Draft Circular on Regulatory Principles for Management of Model Risks in Credit has highlighted the problems of AI/ML algorithms. Algorithmic some times contain bias and bad credit judgments (Fintech Lending Risk Barometer,2024). The report (FinSec: An Emerging Equation between FinTech and Cybersecurity, 2025) mentions about the RBI's Master Directions on Cyber Resilience and Digital Payment Security Controls. These rules stress the need for payment system operators to report incidents, monitor fraud in real time, and follow stricter cybersecurity standards.

(ShaShidhar KJ, 2020) has discussed India’s regulatory sandbox and its policy implications. RBI’s Inter-Regulatory Working Group on FinTech and Digital Banking (2018) has classified AI and robotics as major fintech innovations (AI in Banking A Primer). (Gupta et al., 2024) have analysed the Digital Personal Data Protection Act (DPDP), 2023, outlining its significance for the ethical and lawful deployment of AI systems.

These studies have together explored RBI’s broader fintech regulations. Most of them have acknowledged the intersection between AI and regulatory requirements. But there remains a clear academic gap. No existing study has conducted an exclusive, structured evaluation of RBI’s regulations only for AI-related risks. Similarly, no paper systematically categorizes AI-induced risks from a user-centric perspective.

This study plans to categorize AI induced risk into following two categories. First AI risks affecting consumers, and second AI risks affecting financial institutions.

This structured categorization is intended to support clearer policy analysis. Because many AI risks are mutual in nature and affect both users and institutions simultaneously. By organizing these risks and mapping them against RBI's regulatory frameworks, this study provides an original contribution to the emerging discourse on AI governance in India's fintech sector.

Objectives of the Study

1. To identify AI-induced risks affecting consumers in the fintech sector.
2. To identify AI-induced risks affecting financial institutions.
3. To examine how RBI's existing regulations address these AI-related risks.

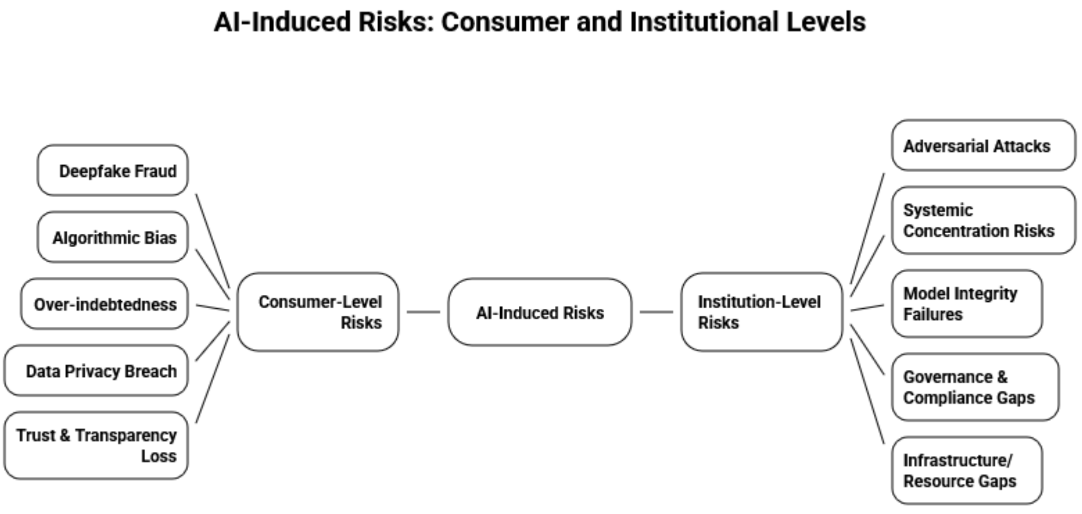
Methodology

This study uses a qualitative document-analysis approach. RBI circulars, Master Directions, committee reports, industry threat assessments, and peer-reviewed articles published between 2017 and 2025 will be analysed to examine how RBI regulations address AI-related risks in the fintech sector. Sources were selected through targeted searches on the RBI website, Google Scholar, SSRN, and open-access institutional repositories. The key words used for searching are as follows AI risk, fintech regulation, model risk, and digital lending guidelines.

Documents that discuss AI/ML risks, fintech vulnerabilities, consumer-protection issues, or regulatory governance in the financial sector were included for analysis. Materials not related to financial AI risks, general AI ethics papers, and outdated fintech reports were not used for evaluations.

RBI's FinTech related documents were reviewed. Policy provisions related to data governance, model validation, cybersecurity controls, outsourcing risks, and consumer-protection requirements in the documents were identified.

3.AI Risks Affecting FinTech Consumer



3.1 Fraud and Identity Theft

Scammers use generative AI to create deepfake videos, audios and documents. These materials are used to bypass security checks and attack the consumers.(FinSec: An Emerging Equation between FinTech and Cybersecurity, 2025) AI tools are able to coordinate highly enhanced phishing and social engineering attacks. This is possible because AI automate personalization information is used to deceive users and steal credentials.(FSB, 2024) AI induced threats are escalated by other risks like SIM card swapping, Man-in-the-Middle (MITM) attacks, and identity theft. Multiple fraud activities have caused financial loss for customers.(A Cybersecurity Agenda for India's Digital Payment Systems Executive, 2019)

3.2 Algorithmic Bias and Financial Exclusion

AI models tend to discriminate consumers in lending, credit scoring, and fraud detection. (Vučinić & Luburić, 2024).Actually system biases present in historical data can lead to the exclusion of certain communities from credit and restrict access to services. (Gaviyau & Godi, 2025).The risk of exclusion happens when AI uses demographic data or surrogate data to assess consumer creditworthiness.(Vipra, 2020)

3.3 Data Privacy and Confidentiality Risks

The deployment of AI systems requires organizations to process vast amounts of consumer data. Storing and processing this amount of information increases concerns related to data privacy, confidentiality, and unauthorized data usage. Consumers are exposed to the risks of poor visibility on data ownership and non-compliance with data protection regulations(Fintech Lending Risk Barometer 2024. Insufficient safe guard of data can cause data breaches and the compromise of sensitive personally identifiable information (PII).(Digital Thread Report 2024).

3.4 Unfair Conduct and Over-Indebtedness

Consumers are exposed to the risk of aggressive marketing and collection practices, such as persistent harassment and deceptive tactics, especially from unauthorized operators, which severely undermines trust(Fintech Lending Risk Barometer 2024). A A distinct risk is indebtedness. Lenders are unable to adequately assess consumers' credit repayment and absorption abilities this leads the customer to become over-indebted.

3.5 Transparency and Trust Erosion

AI models are becoming complex and inexplainable in nature. This nature of AI operates as opaque "black boxes,". Black Boxes complicate regulatory compliance and diminish consumer trust(Anwar et al., 2025). Consumers may also be harmed by the risk of being unaware of loan terms, including processing fees and penal charges, due to insufficient transparency. Erode trust and confidence can also result from unreliable outputs generated by AI.(Saha et al., 2025)

4. AI Risks Affecting FinTech Institutions

4.1 AI-Enabled Operational and Cyber Threats

Threat actors launch highly effective threats like polymorphic malware and AI-enabled phishing attacks. Use of AI for these attacks easily bypass detection. Operational threats mainly include ransomware attacks, Distributed Denial of Service (DDoS) attacks, malware injection, APT, insider threats, supply chain attacks, and API exploits. Use of quantum computing may increase threats to current encryption standards in long term.(Digital Thread Report 2024; FinSec: An Emerging Equation between FinTech and Cybersecurity, 2025)

4.2 Systemic Risk and Concentration

Adopting AI technology can cause systemic risk to financial institutions primarily through third-party dependencies. Service providers are specialized in hardware and cloud services are more prone to such type of risk(FSB, 2024). Reliance on the same few algorithms can amplify procyclicality and market volatility by increasing correlations in trading, lending, and pricing. (FSB, 2024)The complexity and inscrutability of AI underwriting can mask the true risk of loans, especially when combined with securitization, raising the potential for contagion.(Odinet, 2023)

4.3 Model Integrity and Adversarial Attacks

AI integration increases model risk, heightened by the complexity of advanced algorithms, which operate as "black boxes" and hinder audits. Institutions are vulnerable to adversarial attacks that compromise model integrity, such as data poisoning (corrupting training data) and prompt injection (where LLM inputs are manipulated to override safety guardrails).(Anwar et al., 2025) The unreliability of Generative AI, demonstrated by a high number of false positives, poses a continuous operational challenge.(Feyen et al., 2021)

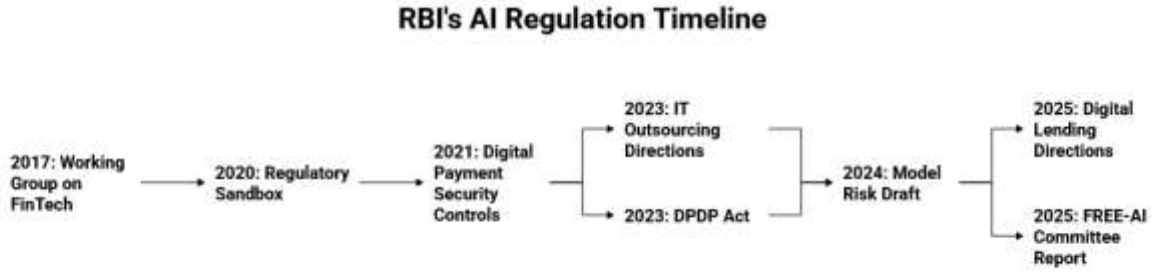
4.4 Regulatory and Governance Failures

Institutions face major risks from non-compliance due to ambiguous and rapidly changing rules. The disaggregation of the financial services value chain makes it challenging to pin down responsibility for mishaps or misdeeds across various service providers. Unregulated activities, such as reliance on Robotic Process Automation (RPA) and Robo advisors, introduce legal responsibility challenges when automated errors occur. Failure to maintain compliance and governance leads to financial loss, reputational damage, and may invite regulatory action.(Fintech Lending Risk Barometer 2024)

4.5 Resource and Infrastructure Gaps

Implementing and maintaining AI systems need a vast amount of computational power and processing capabilities. Operational effectiveness of this system is costly. The industry struggles with a shortage of skilled AI, data science, and cybersecurity professionals. FinTechs often prioritize rapid product releases over secure development. Focusing only on new product launch results in overlooked vulnerabilities and an imbalance between speed and safety.(FinSec: An Emerging Equation between FinTech and Cybersecurity, 2025)

5.Evaluation of RBI Policies and Sources on AI Risk


RBI's AI Regulation Timeline
2017: Working Group on FinTech
2020: Regulatory Sandbox
2021: Digital Payment Security Controls
2023: IT Outsourcing Directions
2023: DPDP Act
2024: Model Risk Draft
2025: Digital Lending Directions
2025: FREE-AI Committee Report

Bellow RBI regulation related to AI in and fintech are evaluated one by one.

Evaluation of RBI Policies on AI Risk in FinTech

5.1 FREE-AI Committee Report (August 2025)

The FREE-AI Committee Report is the most explicit and dedicated source regarding AI risk in the financial sector, providing a comprehensive framework for governance.

The FREE-AI Report explicitly defines comprehensive modern threats, including data poisoning, adversarial attacks, prompt injection, model inversion, model herding, and GenAI hallucinations. It mandates a strong governance structure: requiring Board-approved AI policies for REs, assigning full liability for AI outcomes (Sutra 5), and implementing governance across the entire AI lifecycle. Key mitigation includes performing structured red teaming, augmenting BCPs for model degradation, and establishing a sector-wide AI repository to monitor systemic risks.

However, the report is a set of recommendations (7 Sutras) and not an enforceable regulatory policy, lacking immediate binding technical standards. It notes existing sectoral alignment gaps with the DPDP Act regarding model training practices like synthetic data validation. Furthermore, it emphasizes general governance but fails to provide specific technical standards for mitigating deepfake fraud during processes like V-KYC.(Free AI Commitee, 2025.)

5.2. Draft Regulatory Principles for Management of Model Risks in Credit (August 2024)

This draft focuses on internal model risk management (MRM). It implicitly addresses risks arising from AI/ML models.

The Draft Regulatory Principles for Management of Model Risks in Credit requires that model outcomes should be consistent, unbiased, explainable, and verifiable. It mandates Board-approved governance during the entire model lifecycle. The institution has to also ensure yearly independent validation and review models for bias or discrimination. For outsourced models, REs retains ultimate accountability and must obtain minimum technical documentation.

However, the draft fails to explicitly address AI-specific cyber threats like adversarial attacks or data poisoning. It also lacks binding technical standards for demonstrating explainability (XAI) and does not cover GenAI-specific risks like hallucinations or prompt injection.

5.3. RBI (Digital Lending) Directions, 2025 (May 2025)

Digital Lending Directions mainly focus about consumer protection, accountability, and data governance for digital lending.

The RBI (Digital Lending) Directions, 2025 solve AI risks through strong consumer safeguards. They require need-based data collection with explicit, revocable consent, prohibiting access to resources like contact lists. The policy mandates transparency. The policy prohibits dark patterns to prevent algorithmic manipulation. REs are fully responsible and liable for LSPs' actions.

But the Directions fail to mandate technical controls or testing to secure AI/ML models against integrity threats like data poisoning or adversarial inputs. They also lack explicit requirements for periodic algorithmic fairness audits or specific enforcement methods for ensuring consistent and unbiased AI-driven matching.

5.4. Master Direction on Outsourcing of Information Technology Services (April 2023) & NBFC Outsourcing Guidelines (2017)

These directions address third-party risk management for IT services. Outsourcing services inherently includes cloud and service providers often handling AI models.

Vendor must be careful in outsourcing services related to infrastructure, security, and BCP. Guidelines mandates assessment of concentration risk and ensures RBI’s right to inspect and access the service provider's infrastructure and data. Data integrity and segregation are also required in multi-tenant environments.

The policy fails to mandate AI-specific vendor transparency. Regulations do not ensure disclosure of AI/ML used. They also do not have access to model performance metrics for bias audits. It also lacks explicit ML-specific SLA metrics (e.g., maximum allowable drift) and specialized contingency planning for AI-specific failures like model degradation.

5.5 Master Direction on KYC/AML (Updated August 2025)

This direction addresses fraud and compliance risks in customer onboarding and monitoring.

The KYC/AML Master Direction enables AI use by explicitly allowing appropriate AI technology to ensure V-CIP robustness. It encourages leveraging AI & ML for effective on-going due diligence and transaction monitoring. The policy requires ML/TF risk assessments for new technologies.

The policy does not mandate specific technical safeguards or testing standards for detecting high-risk GenAI-enabled frauds (like deepfakes) during V-CIP. It fails to explicitly address algorithmic bias in AI/ML tools used for customer risk categorization.

5.6. Master Direction on Digital Payment Security Controls (February 2021)

This direction addresses security and fraud across digital payment channels.

The Master Direction on Digital Payment Security Controls addresses AI risks implicitly by mandating a highly evolved fraud monitoring framework and requiring configurations for identifying suspicious behaviour. It promotes resilience through a "secure by design" approach in the ASLC and monitoring for malicious applications.

However, the policy fails to explicitly address GenAI cyber threats, such as AI-enabled malware or sophisticated phishing. It also lacks provisions for protecting internal AI/ML fraud models against model-specific cyberattacks, like data poisoning or evasion techniques.

5.7. Enabling Framework for Regulatory Sandbox (Updated February 2024)

This framework provides a safe environment for testing new technologies.

Innovation Enablement elements in the document permits testing of Artificial Intelligence and Machine Learning applications. It requires applicants to submit plans to mitigate significant risks arising from their FinTech solution.

This document also mandates institution to maintain Customer privacy and data protection standards. Institution must work in compliance with the Digital Personal Data Protection Act, 2023

But the framework does not explicitly mandate adversarial robustness testing or detailed fairness stress tests for AI models before they exit the sandbox. Also there is no mandatory public disclosure of safety test outcomes, although the RBI reserves the right to publish relevant information.

5.8. Working Group Report on FinTech and Digital Banking (November 2017)

This initial report pre-dates the modern AI revolution but identified early algorithmic risks.

The Working Group Report on FinTech (November 2017) acknowledges AI & Robotics as key innovations. AI’s potential to revolutionize data analytics and customer experience was predicted well ahead of the time. It recommends a tiered regulatory philosophy. Supervision varies from "Disclosure" to "Full-Fledged Supervision" mainly based on risk implications.

Because it was published in 2017, the report fails to address modern AI risks like Generative AI, deepfakes, or prompt injection. It also lacks specific governance detail, such as mandatory requirements for AI model lifecycle oversight, bias detection, or explicit explainability metrics.

5.9. Concept Note on Central Bank Digital Currency (October 2022)

The CBDC note touches upon technology and security. It acknowledges that AI integration is unavoidable. It emphasises that CBDC platforms will generate vast data sets and that robust Big Data analytics can support evidence-based policymaking and strengthen AML enforcement. It also states that security must remain the primary design priority from the very beginning of CBDC development.

However, the note overlooks the governance requirements and safeguards needed when autonomous AI agents operate and transact on CBDC infrastructures. It similarly fails to address emerging AI-enabled market risks, such as GenAI-driven manipulation or the heightened systemic volatility that could arise from algorithmic herding within a CBDC-based financial environment.

5.10. Digital Personal Data Protection (DPDP) Act, 2023

The DPDP Act provides overarching data governance highly relevant to AI’s data inputs.

The DPDP Act, 2023 has established legal basis for security safeguards for personal data. Repeat offenders are punished under this act. It enforces privacy and consent principles which includes purpose limitation and Data Principal rights. Facilitation of above is critical for responsible AI training.

However, as a general law, the Act lacks granular technical standards for the financial sector, omitting explicit requirements for algorithmic bias audits or XAI methodologies. It also does not provide explicit guidance on AI-critical practices like the rules for using synthetic data in model training.

5.11. Directions on Managing Risks and Code of Conduct in Outsourcing of Financial Services by NBFCs (2017)

Similar to IT Outsourcing guidelines, this addresses general operational risks.

The NBFC Outsourcing Directions (2017) implicitly manage AI risk by requiring guarding against Reputation Risk (poor service delivery) and Operational Risk (technology failure/fraud). NBFC retains ultimate control and responsibility for the service provider's actions.

The policy fails to mandate specific security protocols for protecting AI/ML models. The policy ignores requirement of due diligence to assess algorithmic fairness or bias within third-party AI systems used for outsourced services.

6.Discussion

The findings of this study highlight a critical divergence in India’s approach to regulating financial technology: the Reserve Bank of India (RBI) has strong instruments addressing governance, liability, and consumer protection, but these measures demonstrate limited engagement with the technical vulnerabilities specific to Artificial Intelligence (AI).

The RBI’s existing regulatory architectures like the Digital Lending Directions (2025) and Outsourcing Master Directions have tried to addresses risks by enforcing strict accountability. RBI documents require explicit consumer consent. Also the regulated entities must retain full responsibility for actions taken by Lending Service Providers (LSPs) or outsourcing vendors. This framework is robust in areas concerning data governance, liability allocation, and consumer consent.

However, the analysis demonstrates a significant regulatory gap concerning technical, model-level safeguards. Data poisoning, prompt injection, deepfake identity fraud, algorithmic bias are most important risks identified this document. RBI policies largely fail to mandate specific technical controls or testing related to the above risk.

There is a lack of binding requirements for core AI governance practices. In RBI’s guidelines mandatory algorithmic fairness audits, model robustness testing, and specific methodologies for explainability (XAI) are not existing. The intent for unbiased and responsible AI use is clear but there is the lack of technical standards. The gap limits the ability of the framework to mitigate the rapidly evolving and sophisticated threats caused by modern AI and Generative AI systems.

7.Conclusion

This study provides a structured evaluation of the Reserve Bank of India's (RBI) regulations related to AI risks in the fintech sector. By mapping categorized threats affecting both consumers and institutions against existing policies, the research confirmed the presence of a robust foundational layer of governance. This framework has successfully enforced strict accountability. It also requires explicit consumer consent and mandates due diligence for outsourcing risks.

RBI framework lacks binding requirements for key mitigation practices. RBI has to frame policies regarding threads like adversarial attacks, deepfake fraud, and algorithmic bias leading to financial exclusion. This research has identified the above imbalance in RBI framework.

RBI must evolve its policies by transforming generalized governance principles into enforceable technical standards. Future regulatory action should focus on mandating model robustness testing, specific methodologies for explainability (XAI), and mandatory algorithmic fairness audits. This is essential to counter the rapidly evolving and sophisticated systemic risks due to modern Generative AI systems.

REFERENCES

1. *A Cybersecurity Agenda for India's Digital Payment Systems Executive*. (2019). https://www.gatewayhouse.in/wp-content/uploads/2019/10/Digital-Payments_FINAL.pdf
2. *AI in Banking A Primer*. (n.d.). Retrieved December 1, 2025, from https://www.idrbt.ac.in/
3. Anwar, S., Sayedahmed, N., & Pradeep, S. (2025). AI-driven risk management in online financial transactions: Enhancing cybersecurity in the fintech ERA. *International Journal of Innovative Research and Scientific Studies*, *8*(4), 328–335. https://doi.org/10.53894/ijirss.v8i4.7784
4. *Artificial Intelligence in Financial Services*. (2025). https://reports.weforum.org/docs/WEF_Artificial_Intelligence_in_Financial_Services_2025.pdf
5. *digital Thread Report 2024*. (2024). https://www.cert-in.org.in/PDF/Digital_Threat_Report_2024.pdf
6. Feyen, E., Frost, J., Gambacorta, L., Natarajan, H., & Saal, M. (2021). *BIS Papers No 117 Fintech and the digital transformation of financial services: implications for market structure and public policy*. www.worldbank.org
7. *FinSec: An emerging equation between FinTech and cybersecurity*. (2025). pwc.in
8. *Fintech Lending Risk Barometer 2024 Understanding the perception of risks in the Fintech lending sector in India*. (n.d.).
9. *Free AI Committee Report*. (2025). https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/FREEAIR130820250A24FF2D4578453F824C72ED9F5D5851.PDF
10. FSB. (2024). *The Financial Stability Implications of Artificial Intelligence*. www.fsb.org/emailalert
11. Gaviyau, W., & Godi, J. (2025). Emerging Risks in the Fintech-Driven Digital Banking Environment: A Bibliometric Review of China and India. *Risks*, *13*(10), 186. https://doi.org/10.3390/risks13100186
12. Gupta, C. M., Kaur, G., & Yuliantiningsih, A. (2024). Fin-tech Regulations Development, Challenges, and Solutions : A Review. *Jurnal Dinamika Hukum*, *24*(1), 124. https://doi.org/10.20884/1.jdh.2024.24.1.4074
13. Kagalwala, H., Paruchuri, S., Josyula, H. P., Anand Kumar, P., & Al Said, N. (2024). AI-Powered FinTech: Revolutionizing Digital Banking and Payment Systems. In *Journal of Information Systems Engineering and Management* (Vol. 2025, Issue 33s). https://www.jisem-journal.com/https://www.jisem-journal.com/
14. Kumar, P. (2024). AI-Powered Fraud Prevention in Digital Payment Ecosystems: Leveraging Machine Learning for Real-Time Anomaly Detection and Risk Mitigation. In *Journal of Information Systems Engineering and Management* (Vol. 2024, Issue 4). https://www.jisem-journal.com/
15. Odinet, C. K. (2023). *FINTECH CREDIT AND THE FINANCIAL RISK OF AI*. https://www.cbsnews.com/news/the-united-states-of-indebted-america/;
16. Saha, B., Rani, N., & Shukla, S. K. (2025). *Generative AI in Financial Institution: A Global Survey of Opportunities, Threats, and Regulation*. https://doi.org/10.48550/arXiv.2504.21574
17. ShaShidhar KJ. (2020). *Regulatory Sandboxes: Decoding India' s Attempt to Regulate Fintech Disruption*.
18. Vipra, J. (2020). *Regulating AI in the Finance Sector in India*.
19. Vučinić, M., & Luburić, R. (2024). Artificial Intelligence, Fintech and Challenges to Central Banks. *Journal of Central Banking Theory and Practice*, *13*(3), 5–42. https://doi.org/10.2478/jcbtp-2024-0021