VOLUME 6 | ISSUE 3

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

ARTIFICIAL INTELLIGENCE IN FINANCE: CYBER LAWS AND AI-DRIVEN BANKING FRAUDS

- Deyona Shajees*

Abstract

The Artificial Intelligence (AI) has revolutionized the banking business worldwide bringing efficiency in the areas of fraud detection, risk evaluation, and customer services. The negative aspect of it is, however, the increasing complexity of AI-based crimes. Genuine AI applications like deepfakes, synthetic identities, and voice cloning are currently used by fraudsters bypassing verification protocols to impersonate a real customer or official. Such nefarious applications of AI have caused major financial and reputational losses to banks, not mentioning the psychological trauma of customers. In addition, there are algorithmic biases and privacy concerns that make fraud detection mechanisms difficult. The paper discusses the transformations of AI in the defensive and offensive aspect of financial cybersecurity, specifically the legal, ethical, and policy issues of AI-driven banking fraud. In a comparative discussion of cyber laws in the world and the IT Act of India, the U.S. Computer Fraud and Abuse Act, and the European Union AI Act, this study highlights the necessity of a unified international regulation and ethical use of AI. Real-world vulnerabilities and responses have been represented through case studies. The results show that although AI-powered innovations strengthen financial systems, they also restructured fraud, which requires active regulation, algorithmic openness, and inter-sector cooperation to defend consumer rights and confidence in online financial services.

Keywords: *Artificial Intelligence (AI); AI-driven Banking Frauds; Generative Adversarial Networks (GANs); Large Language Models (LLMs); Explainable AI (XAI); Know Your Customer*

*Student at Christ (Deemed to be University) Pune, Lavasa Campus

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

https://www.ijalr.in/

(KYC); Information Technology Act, 2000; Digital Personal Data Protection Act, 2023 (DPDP Act); Algorithmic Bias; Financial Cybersecurity.

INTRODUCTION

Artificial Intelligence (AI) is a groundbreaking technology in banking to detect fraud, to control risks, and to become more personalized, but it is also the new means of enhancing advanced criminal activities such as deepfakes and voice cloning to become a representative of an official or a client. Generative AI is used to commit fraudsters who bypass biometric KYC (Know Your Consumer), commit social engineering using LLMs (Large Language Model), and generate synthetic identities, causing massive debt such as the 45 crores in India in 2024 and 2025[1]. Also, new reports found out a significant uprising in AI- enabled financial crime in India. This resulted with a total loss reaching over ₹22,800 crore in 2024 alone[2].Suchattacks destroy customer trust, result in financial distress of identity theft and unauthorized transactions, and flood the detection systems with emerging tactics. Banks experience false negatives which enable fraud slippage, algorithmic biases in identifying legitimate activity, and privacy concerns because of huge sensitive data-sets. Current cyber regulations such as the Information Technology Act 2000 in India are not sufficient to deal with AI-related threats, such as deepfakes, and do not include a basis to hold the accountable in the case of cross-border jurisdiction. The present paper assesses the twofold role of AI in banking practices, regulatory loopholes, ethical issues, and introduces a cohesive system uniting the law, ethics, and technology to reduce risks and promote safe AI implementation.

AI'S DUAL IMPACT ON BANKING

The entire banking processes do have Artificial Intelligence (AI) that contributes to increased efficiency in revealing fraud, identification and management of customers, and risk assessment[3], and, unintentionally, also provokes vulnerabilities that attackers exploit in their antagonistic

[1]Volodymyr Zverev et al., Artificial Intelligence and Cybercrime: New Challenges and Prospects for Legal Regulation, 1 Contemp. Issues in Artificial Intelligence 1 (2025).
[2]E. Oztemel& Muhammed Işık, A Systematic Review of Intelligent Systems and Analytic Applications in Credit Card Fraud Detection, 25 Applied Sci. 1 (2025).
Arushi Mehta, Impact of Technological Advancements on Banking Frauds: A Case Study of Indian Banks, 7 Int'l J. Res. Fin. & Mgmt. 261 (2024).
[3]Kamal Kumar Hindolia, Artificial Intelligence in Financial Services: Revolutionizing Risk Assessment and Fraud Detection in Modern Banking, 7 Int'l J. for Multidisciplinary Research 1 (2025).

actions and inherent bias. Even though machine learning (ML) and deep learning (DL) algorithms could be applied to detect the threats ahead of time, the integration of the machine learning algorithms into the primary functional spheres could demonstrate the weak points of the systems, and the traditional protection mechanisms lose their benefits to the AI-powered threats[4]. The case of CNN-RNN-LSTM hybrids suggests that the multi-agent DRL is a better predictor of transaction risk because it can work with large datasets in a highly specific and adaptive way of learning than an alternative rule-based system.

However, by introducing adversarial examples to training data, fraudsters lead to model drift and evasion, and overreliance on simulated data, which is not governed by the dynamics of the real world, accelerates this. Facial and voice recognition in AI is bonded by Know Your Customer (KYC) and biometrics Onboarding, to make compliance easier, yet the more sophisticated networks produced by GANsare synthetic faces and identities that are impossible to detect as lively, and deployed in generative adversarial networks (GANs). One such 2024 Indian fintech casebased on deepfakes and AI-generated paperwork, scammers registered accounts and obtained 45 crores in quick and easy loans without being automatically screened and without a manual audit since the algorithms rely on them. Prospective analytics is used in risk assessment to score credit and liquidity management, which is less reactive and more proactive in its measures, yet the results of past discrimination and lack of awareness to high-risk fraud patterns still persist. The impact of such an opaque state as the underestimation of new risks, such as money laundering networks.[5]

Customer-facing AI, including chatbots and phishing filters, that work on natural language processing (NLP), can be handy to enhance the responsiveness of the services, yet big language models (LLMs) can enable fraudsters to build adaptive and hyper-personalized fraud in the shape of official messages. The XG-Boost model is currently very precise in predicting fraud in online transactions, and in the circumstances of real-time social engineering by using the help of LLMs, psychological indicators are taken into account, and filters are outsmarted in mobile banking

[4]Praveen Sivathapandi, Multi-Agent Model Based Risk Prediction in Banking Transaction Using Deep Learning Model, J. Critical Reviews 1 (2024).
[5]Mohamed Kamal Aldin Ismaeil, Harnessing AI for Next-Generation Financial Fraud Detection: A Data-Driven Revolution, 3 J. Ecohumanism 811, 821 (2024).

programs[6]. Case Study: Punjab National Bank Fraud[7] (2018, AI Evolutions) -Previously a 1.8 billion letter of credit fraud, which involved a classical collusion, recent RBI (2024) reports of AI adaptations with deepfakes posing as authorities to get unauthorized approvals and reveal the laxity in the AI-based controls, the use of AI technology under the IT Act Section 66C[8] to convict people of identity theft is a controversial discussion[9]. There must be equal control in such duality to be able to use the benefits of AI and to avoid the usage of AI as a weapon.

EVOLUTION OF AI-DRIVEN BANKING FRAUDS

Outlook of AI-Based Banking Frauds. The creation of AI-based frauds is not stagnant and has been exploited by the management of banks that heavily rely on automated processes each day to conduct their operations and, instead of a basic phishing attack, now has advanced to more sophisticated and versatile attacks, which mimic regular processes[10]. Fraudsters can now generate highly realistic face videos and fake documents, with the assistance of Generative Adversarial Networks (GANs), specifically, StyleGAN3, that satisfy and pass remote Know Your Customer (KYC) authentication during opening accounts and instant loan application[11]. An especially dangerous example of an over-reliance on AI screening is online onboarding is an Indian fintech company that lost 45 crores after two criminals used deepfake video and identity papers made using AI to pass automated compliance checks and manual audits.

Neural text-to-speech voice cloning systems like Glow-TTS and FastSpeech2 can reproduce the speech of a person, intonation, and accents of a person or a group using a simple recording of the voice, directly targeted at voice biometrics in call centres or transaction authorizations. Reality Defender stress tests indicated that 75 percent of banking voice authentication systems failed to operate against the audio equivalent of such cloning in an adversarial setting, which demonstrated weaknesses in mobile banking call centres where consumers allow transfers of

[6]Rachna Rathore et al., Fraud Detection in Online Transactions Using Machine Learning, in 2024 1st Int'l Conf. on Advances in Computing, Comm. & Networking (ICAC2N) 1 (2024).
[7]P.N.B. Staff Assn. v. Union of India, (2019) 2 S.C.C. 228 (India).
[8]Information Technology Act, No. 21 of 2000, § 66C (India).
[9]Gobi Natesan, Prevention of Cyber Frauds in the Banking Sector, Int'l Sci. J. Eng'g & Mgmt. 1 (2024).
[10]Volodymyr Zverev et al., Artificial Intelligence and Cybercrime: New Challenges and Prospects for Legal Regulation, 1 Contemp. Issues in Artificial Intelligence 1 (2025).
[11]Arushi Mehta, Impact of Technological Advancements on Banking Frauds: A Case Study of Indian Banks, 7 Int'l J. Res. Fin. & Mgmt. 261 (2024).

high value to be authorised. This is a combined system with the day- to-day operations of the bank where day to day impersonation of the bank officials or account holder can be done. The risks of threats also rise directed at Large Language Models (LLMs), which may misuse the opportunity to steal unprotected and published customer data to generate hyper-personalized phishing campaign messages, introduce pressures of urgency and authority bias to emails, SMS, or chat interfaces, and imitate a real support team in the bank.[12]

The adaptive fraud chatbots enhance the response in real-time bypassing the NLP-based filters within the customer apps. These tricks are more advanced than defence; in the example of Rathore et al. (2024), the XG-Boost model will identify transaction fraud with 91% accuracy, but will not be able when it encounters a social engineered by dynamic LLMs. Case Study: Deepfake Scam of Hong Kong Bank (2024) - Fraudsters impersonated executives using AI-cloned voices to defraud a finance worker of 25 million by taking 15 phone calls and circumventing multi-factor authentication; not Indian, but trends are similar to those reported by RBI in UPI scams, where similar voice deepfakes were used to facilitate 1,500 crores cheating under the IT Act Section 66D[13] despite the evidentiary hurdle. KYC failures, voice risks by helpdesks, and LLM scams enter apps and all of those overwhelm a static defence to drive account takeovers.

REGULATORY CHALLENGES

The Indian cyber law, which is mainly covered under the Information Technology Act, 2000 (IT Act)[14], alongside the Bharatiya Nyaya Sanhita, 2023 (BNS)[15], Bharatiya Sakshya Adhiniyam, 2023 (BSA)[16], Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS)[17], Digital Personal Data Protection Act, 2023 (DPDP Act)[18], the sectoral guidelines of the Reserve Bank of India (RBI) and the Securities and Exchange They enforce penalties on personation, manipulation of data and negligence but do not assign explicit liability on the AI systems themselves, as though they are

[12]Rachna Rathore et al., Fraud Detection in Online Transactions Using Machine Learning, in 2024 1st Int'l Conf. on Advances in Computing, Comm. & Networking (ICAC2N) 1 (2024).
[13]Information Technology Act, No. 21 of 2000, § 66D (India); Gobi Natesan, Prevention of Cyber Frauds in the Banking Sector, Int'l Sci. J. Eng'g & Mgmt. 1 (2024).
[14] Information Technology Act, No. 21 of 2000 (India).
[15] Bharatiya Nyaya Sanhita, No. 45 of 2023 (India).
[16] Bharatiya Sakshya Adhiniyam, No. 47 of 2023 (India).
[17] Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023 (India).
[18] Digital Personal Data Protection Act, No. 22 of 2023 (India).

tools like malware, and leaves the question of whether the creator of a harmful model (e.g. a fraud-optimizing GAN or StyleGAN3), the bank that does not deploy an effective detector, or the user who does so, as the primary responsibility, which creates prosecutorial ambiguities in cross-border scams involving foreign-hosted open-source LLM[19] and creates gaps in the investigation process.

i. Bharatiya Nyaya Sanhita, 2023 and Information Technology Act, 2000

Section 66C (identity theft through electronic signatures or unique ID)[20] and 66D (cheating through personation using computer resources)[21] of the IT Act directly apply to the AI-driven banking frauds, including deepfake voice cloning in UPI scams where the criminal impersonates a relative to encourage transfers or creation of forged electronic records under Section 336[22], and related provisions such as Section 43A[23] which imposes liability on the human perpetrator of the fraud, and Section 318(cheating that dishonestly induces delivery of property)[24] and Legal issues are also created by their technological impartiality, in that these parts presuppose identifiable human agency, but not autonomous AI actions, or hold model designers responsible, who facilitate widespread fraud by means of general-purpose open-source utilities, showing the creation of specific abetment, conspiracy, or knowledge under general principles, which is factually difficult to achieve in decentralized AI systems[25]. In the groundbreaking cases such as Avnish Bajaj v. state, a ruling by State (Bazee.com, 2005, Delhi HC)[26] inferred IT Act Section 67 to create the type of intermediary liability on platforms hosting obscene content, a concept applied in 2024 to cyber-fraud cases involving AI-related UPI scams, but fails in situations where generative AI has been systematically abused to make providers liable such as in reported cases of voice-cloning in the city of Delhi but no developer or payment gateway is directly responsible.

[19]Tim Maurer & Arthur Nelson, International Strategy to Better Protect the Financial System Against Cyber Threats, Carnegie Endowment for Int'l Peace (2020).
[20] Information Technology Act, No. 21 of 2000, § 66C (India).
[21] Information Technology Act, No. 21 of 2000, § 66D (India).
[22] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 336 (India).
[23] Information Technology Act, No. 21 of 2000, § 43A (India).
[24] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 318 (India).
[25]Tim Maurer & Arthur Nelson, International Strategy to Better Protect the Financial System Against Cyber Threats, Carnegie Endowment for Int'l Peace (2020).
[26]Avnish Bajaj v. State, 2005 Cri. L.J. 2301 (Del.)(India).

Equally, in the case of Shreya Singhal v. Union of India (2015, Supreme Court)[27], Section 79 safe harbour safeguards were enforced against passive intermediaries, which adds an additional layer of protection to AI platforms unless proactive monitoring is not performed and the failure of AI detection is not punished beyond dubious negligence claims.

ii. Bharatiya Sakshya Adhiniyam, 2023 and Bharatiya Nagarik Suraksha Sanhita, 2023

Section 61-63 of BSA[28] provide that AI-generated banking logs, transaction emails, deepfake videos, or digital signatures are admissible as primary evidence on par with paper records, that custodian certificates must be provided under Section 62[29] to explain how they produced the records to maintain chain-of-custody of manipulated information, and that integrity proofs such as hash values, metadata, or digital signatures under Section 63[30] are rejected to accept tampered records. These features create regulatory difficulties by the obvious lack of any AI-specific forensic guidelines such as standardized GAN detectors, deepfake watermark detectors, or reliability metrics of synthetic media such that, despite insufficient hardware infrastructure, judicial digital literacy gap, or lack of real-time extraction methods of transient encrypted banking records by police at the local level, a subordinate court may face continual challenges in evidentiary thresholds with hyper-realistic deepfakes that parody a real transaction video or audit trail, which can be made worse by incompetence or insufficient There is no central body, such as a proposed Deepfake Detection Centre, to standardize AI evidence usage in financial frauds, which evidently creates a looming evidentiary crisis where high-risk AI products do not have rebuttable presumptions, and this is the core of the issue in doctrinal critiques of BSA amendments, e.g., in ongoing Kerala deepfake UPI prosecutions (2023), courts have had difficulties relying on Section 63 to prove cloned voice recordings in the absence of specialized technology.[31]

iii. RBI and SEBI Guidelines

[27]Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).
[28] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 61-63 (India).
[29] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 62 (India).
[30] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63 (India).
[31]Bich Tran, Cybersecurity in Vietnam: Challenges and Opportunities in an Era of Digital Transformation, East-West Center (2025).

RBI Master Directions on Information Technology Governance, Risk, Controls, and Cybersecurity (Directions No. RBI/2023-24/123)[32] requires banks, NBFCs, and payment system operators to use board-level IT supervision, AI/ML risk analysis of core processes such as digital lending and fraud detection, due diligence of third-party vendors with contractual security provisions, penetration testing, audit logs, and incident reporting (6 hours), where SEBI Cybersecurity and Cyber Resilience Framework[33](Circular No. The lack of cross-border enforcement measures against AI-hosted in foreign countries or GAN systems that drive scams, as well as explicit provisions to establish strict liability on AI detection failures, restricting recourse to supervisory penalties, fines, or business restrictions instead of direct victim compensation, and the inability to clarify the boundary between banks and AI vendors when synthetic identity frauds circumvent KYC[34], is all apparent in reports on2,145 crore UPI fraud losses in 2022-2025 in the reports of RBI itself. In reality, such instances as the 2024 Mumbai synthetic loan scam, when AI-generated accounts passed bank verification, have been prosecuted, with BNS cheating alone and no RBI considering the ancillary liability of AI vendors, highlighting the reactive nature in the guidelines to AI responsibility.

iv. Digital Personal Data Protection Law, 2023

The DPDP Act[35] makes banks and fintech Data Fiduciaries, requiring verifiable consent, requiring purpose limitation, requiring security by design, requiring minimum data, and requiring notification of breaches within 72 hours of KYC biometrics or transaction data potentially scraped to train fraud-enabling AI models, and imposing non-compliance penalties of up to250 crore administered by the Data Protection Board. Weaknesses in regulation These are regulatory weaknesses in the fact that it concerns real personal data, and does not cover AI-generated synthetic identities that combine fabricated information with partial real information to circumvent privacy gates in credit scoring or onboarding[36], where it would provide no clear

[32]Reserve Bank of India, Master Directions on Information Technology Governance, Risk, Controls, and Cybersecurity, Directions No. RBI/2023–24/123 (Oct. 19, 2023).
[33]Securities and Exchange Board of India, Cybersecurity and Cyber Resilience Framework, Circular No. SEBI/HO/ITD2/ITD2_POD2/P/CIR/2023/XXX (2023).
[34]Tim Maurer & Arthur Nelson, International Strategy to Better Protect the Financial System Against Cyber Threats, Carnegie Endowment for Int'l Peace 23–45 (2020).
[35] Digital Personal Data Protection Act, No. 22 of 2023 (India).
[36]Jeffrey Gottfried et al., Online Scams and Attacks in America Today, Pew Research Center (July 2025).

liability framework in the event of an exploitative use of artificial datasets, nor would it be clear whether banks, vendors of AI, or processors would be held responsible of such exploitations of privacy-related banking defenses as the number of identity thefts enabled by such evasions increases. Indicatively, in reported 2025 synthetic identity epidemics at risk of 70,000 crore, DPDP implementation was still laggard syndrome as the regulators debated whether morphed profiles would be regarded as personal data with victims having no specific data protection under the BNS/IT Act.[37]Comprehensively, these frameworks require selective reforms, including BSA amendments of AI provenance standards, criminalization of models that optimize fraud under the IT Act, results-oriented detection liabilities with RBI / SEBI requirements, and inclusion of synthetic data in DPDP, to establish endemic integrity in the AI banking fraud ecosystem.

TECHNOLOGICAL AND ETHICAL PROBLEMS

There is a serious ethical and technological dilemma of implementing AI in banking that further exposes the risk of fraud through obscurity, bias of algorithms, loss of privacy, and accountability[38] in day-to-day activities, including fraud detection, risk detection, and risk assessment. The black box models of deep learning that are commonly applied in transaction monitoring and anomaly detection do not show how decisions are reached and can therefore not be interpreted[39], which is not in line with the 2024 Master Directions on cybersecurity of the mandatory compliance of RBI with an audit trail. Explainable AI (XAI) techniques to demystify the predictions are recommended[40], though only a small number of these have been used, and regulators and banks can no longer verify flagged transactions and challenge erroneous outputs.

The discriminatory impacts of biased training information algorithms, such as unfair loan rejection or being unaware of red flags of fraud[41], are encouraged by encouraging the practices that are a consequence of discriminatory principles against people of colour; eroding trust and supporting elaborate escapades. The consequences of prejudices in the AI credit scoring model

[37]Bich Tran, Cybersecurity in Vietnam: Challenges and Opportunities, East-West Center (2025).
[38]Azeez Olanipekun Hassan et al., Cybersecurity in Banking: A Global Perspective, 5 Comp. Sci. & Info. Tech. Res. J. 41 (2024).
[39]Gobi Natesan, Prevention of Cyber Frauds in the Banking Sector, Int'l Sci. J. Eng'g & Mgmt. 1 (2024).
[40]Mohamed Kamal Aldin Ismaeil, Harnessing AI for Next-Generation Financial Fraud Detection, 3 J. Ecohumanism 811 (2024).
[41]Ahmad Mustapha & Anupa Sinha, Cyberfraud in the Nigerian Banking Sector, 9 Int'l J. Innovative Sci. & Res. Tech. 171 (2024).

trained on biased information are captured,[42]where they indicate that by compelling the underrepresented forms of fraud to evade detection, and legitimate minority transactions to be have excessive alerts, the biases of the AI credit scoring models amplify the faults, which are indicative of fairness issues within the interactions with the customers in general. The lack of governance implies that opaque models introduce obstacles to bias auditing, which generate the issue of fairness in AI-based financial decision-making.

What makes the privacy concerns of the Digital Personal Data Protection Act, 2023 (DPDP Act) even more concerning is the fact that AI systems are fed collections of the information about the customer to conduct KYC, biometrics, and behavioural analytics to produce synthetic identities without necessarily stealing the data. A high level of aggregation of data will lead to a higher probability of abuse by insiders or a cyberattack, which is not within the DPDP consent norms and exposes a customer to identity theft in the daily conduct of the company, including the approval of apps. Sivathapandi (2024)[43] finds fault with the overtrained simulated datasets in multi-agent DL models that works well in the lab at 94 percent accuracy, but does not work in practice where the technology is confronted with an adaptive threat, and this concept exposes the vulnerability of technology. The responsibility issue is unsolved: the issue of liability in AI mistakes is not who is going to be liable: banks, vendors or developers; when the risk assessment is not able to evaluate deepfake loans or chatbots are not able to filter phishing? There are gaps in ethics in terms of regaining the trust of the consumers after the fraud, and there are no frameworks when the dual-use aspect of AI shares the responsibility. In the Case Study of HDFC Bank Data Breach (2023)[44] - A cyberattack has disclosed 15M customer records, which resulted in phishing through AI; however, despite the IT act section 66 accusation, was it ethically correct to bias AI recovery models later, but DPDP gaps in AI data processing and moral limits in banking AI are now demanded. Such problems need unified reforms so as to keep technology and ethical demands aligned.

FRAMEWORK PROPOSAL AND RECOMMENDATIONS

[42]E. Oztemel& Muhammed Işık, A Systematic Review of Intelligent Systems, 25 Applied Sci. 1 (2025).
[43]Praveen Sivathapandi, Multi-Agent Model Based Risk Prediction, J. Critical Reviews 1 (2024).
[44]Kamal Kumar Hindolia, Artificial Intelligence in Financial Services, 7 Int'l J. for Multidisciplinary Research 1 (2025).

In order to curtail AI-enhanced banking frauds, the current paper will suggest a sensible multi-level structure that will form the foundation of the balance between the legal, ethical, and technological pillars, which directly address the gaps found in the governance, transparency, and adaptive defences as specified in the literature on regulatory lags, evidentiary crisis, and institutional vulnerability[45]. This comprehensive solution encourages secure AI usage in banks in the modern environment and enhances protection against deepfakes, voice cloning, and scams organized with the help of AI, keeps regulatory and ethical standards, and maintains customer trust in the long term due to proactive efforts instead of reactive enforcement.

i. Technological Pillar

Such real-time fraud detection through deployment of Explainable AI (XAI) models integrated with human-AI hybrid systems can produce interpretable decision rationales such as scores of feature importance of transaction anomalies such as unusual UPI velocities or geolocation deviations, and is directly aligned to the developing principles of FREE-AI through which explainable AI models must provide auditable explanations to regulators and the judiciary.[46]Adaptive deepfake and synthetic identity defences are based on federated learning networks of banks, where the models are trained on siloed data to meet data localization requirements without privacy loss, and are enhanced with multi-modal biometrics, which combine facial liveness detection (investigating blink patterns and texture artifacts), voice authentication (detecting spectrographic inconsistencies in cloned audio) and behavioural biometrics (following keystroke rhythm patterns and device tilt patterns) which have been shown to neutralize GAN-based KYC evasions with lab experiments. Strict constant retraining on anonymous real-world fraud data on shared registries such as the Central Fraud Registry of RBI counteract adversarial overfitting, using methods including differential privacy and robust optimization to resist advanced attacks by more advanced tools such as StyleGAN3, and so does not introduce latency to large-scale digital transactions.[47]

[45]Jeffrey Gottfried et al., Online Scams and Attacks in America Today, Pew Research Center (July 2025) (discussing institutional vulnerabilities in AI-driven fraud governance).
[46]Mohamed Kamal Aldin Ismaeil, Harnessing AI for Next-Generation Financial Fraud Detection: A Data-Driven Revolution, 3 J. Ecohumanism 811, 818–20 (2024) (recommending XAI for regulatory compliance).
[47]Praveen Sivathapandi, Multi-Agent Model Based Risk Prediction in Banking Transaction Using Deep Learning Model, J. Critical Reviews 1 (2024) (federated learning and multi-modal biometrics for KYC).

ii. Legal Pillar

The Information Technology Act, 2000, should be amended to incorporate AI-specific principles of evidencing, specifying the forensic standards of Bharatiya Sakshya Adhiniyam, Sections 61-63, such as a compulsory extraction of embedded watermarks, hash audit anchored by blockchain and certified toolkit to analyse GAN provenance, aiding in the accelerated admissibility of synthetic banking artifacts and addressing chain-of-custody challenges in litigation involving fraud[48]. RBI must issue a set of specific AI regulation standards that require extensive audits of vendors (including the record of model provenance and performance thresholds), compulsory insurance of detection failures with tiered victim compensation limits, and cross-border enforcement measures modelled after the mutual legal assistance provision in the Budapest Convention[49] adjusted to the sovereignty imperatives of India through bilateral agreements to allow quick preservation of offshore LLM records[50], subscriber tracing and coordinated shutdown of global scam systems. This harmonized law would break the jurisdictional siloes with the interpole cybercrime databanks[51] to facilitate the smooth flow of data and prevent the escalation of fraud, especially when UPI losses exceeded2,145 crores through the international orientation of proactive legislation instead of local reaction.

iii. Ethical Pillar

Require bias audits, publish transparency of algorithms, and independent ethical oversight panels - in conjunction with the Digital Personal Data Protection Act, 2023[52] would ensure fairness of AI-mediated risk determination, and customer interactions, and force banks to publish annual transparency reports with performance measures such as equalized odds ratios, calibration curves by different demographic groups, and justifications of denials reasons behind credit or transaction blocks. Strict yearly fairness assessments, applying systems like IBMs AIF360 to investigate cross-sectional bias within caste-gender proxies or regional dialect in fraud scoring, helps minimize discriminatory false positives- such as groups of low-income users, particularly

[48]Tim Maurer & Arthur Nelson, International Strategy to Better Protect the Financial System Against Cyber Threats, Carnegie Endowment for Int'l Peace 34–42 (2020) (discussing blockchain forensics).
[49]Council of Europe, Convention on Cybercrime (Budapest Convention), Nov. 8, 2001, E.T.S. No. 185.
[50]Cristos Velasco, Cybercrime and Artificial Intelligence: Overview of International Organizations, 23 ERA Forum 109 (2022).
[51]INTERPOL, Global Cybercrime Analysis 2024: Financial Fraud Networks (2024).
[52]Digital Personal Data Protection Act, No. 22 of 2023 (India).

low-represented data pools- and establish effective redress mechanisms, such as algorithmic appeals, expedited human overrides, and special compensation funds to address the misuse of AI, and helps repair confidence fractured by black-box failures[53]. This pillar encourages symbiotic co-operation between technologists, legislators, and financial institutions, by instilling RBI-approved behaviours such as lifecycle ethical monitoring and certification badges to create future-focused resilience[54], which makes the Indian banking industry a global leader of human-oriented AI governance.

CONCLUSION

Although the mass adoption of Artificial Intelligence within the financial sector has undoubtedly triggered revolutionary productivity gains within fraud analysis, risk analysis, and customer customization, it has also spawned an equal and opposite reaction within an underworld of sophisticated crime, as typified by deep forgeries, voice hacking, virtual identities, and LLM-driven social engineering attacks. It has been the task of this research paper to methodologically dissect and analyse these dual consequences arising out of AI adoption and demonstrate how generative adversarial networks, exemplified within StyleGAN3 and NTTS models, have adapted biometric-based Know-Your-Customer verification systems, thus enabling an amount worth ₹22,800 crore in 2024 alone as quantified due to fintech onboarding violations and UPI impersonation attacks. Within this unfolding lineage of threats, as these have progressed from static phishing attacks to highly adaptive and hyper-targeted attacks, it becomes unequivocal that there arises a highly prejudicial asymmetry within an immune response reliant on ML models for defence, as typified within XG-Boost and CNN-RNN-LSTM hybrids that have achieved a 94 percent accuracy rate within lab settings.

The regulatory gaze highlights large gaps within cyber-law as it relates to India. The Information Technology Act, 2000, as read with Sections 318-319 and 336 of Bharatiya Nyaya Sanhita (BNS), and Sections 61-63 of Bharatiya SakshyaAdhiniyam (BSA), provides technologically impartial avenues for enforcement against personation and electronic forgery but falls short on attributing culpability within AI networks, be it developer, deploying bank, or end-user, within

[53]K. Prabhu Rajasekar & D. Vezhaventhan, AI-Based Fraud Detection for Telecom Systems (2024).
[54]Saurabh Kumar, Impact of Artificial Intelligence on Customer Experience in Indian Banking, 15–20 (2025) (discussing RBI ethical monitoring).

cross-border deployments of LLMs and gaps in LLM evidence due to ungalvanized GAN-forensics. RBI's 2024 Master Directions and SEBI's CSCRF stipulate vendors' audits and resilience requirements but resist strict liabilities on detection failure and Budapest Convention-compliant treaties, and within this framework, though enabling actual data safeguarding via the Digital Personal Data Protection Act, 2023, it does so without addressing synthetic data and thus continues with attributions from Avnish Bajaj vs. State (2005) and Shreya Singhal vs. Union of India (2015). And in turn, it continues to be exacerbated by technologically ethical crises within black boxes that violate RBI trace requirements, datasets imbued with discriminatory norms that introduce false positives on rural transactions, and internal data aggregation that spawns internal traits vulnerable to insider threats, as seen with HDFC 2023 and Punjab National Bank developments.

To tackle this challenge, it seems that a proactive approach will be facilitated through the suggested three-fold framework: technological, legal, and ethical. From a technological perspective, with the convergence of Explainable AI or XAI with federated learning and multi-modal biometrics, a reliable and explainable defence strategy would be achieved and retaught via RBI's Central Fraud Registry against StyleGAN3 attacks with zero latency. From a legal perspective, amendments within the Information Technology Act enabling BSA-embedded watermark extraction, RBI vendors' assurances, and bi-national enforcement agreements would address domain-wise inconsistencies, obliterating threats associated with RS 70,000 crore 'synthetic Identities'. From an ethical perspective, with bias audits driven by DPDP and involving AIF360, transparency model cards, and redress pools, there would be equity. Finally, this paradigm moves beyond remedial measures and envisions a complementary paradigm on governance itself. It becomes an imperative for governments and regulatory bodies to emphasize these changes and thus avert an evidence crisis. It becomes an area for further research and development, and a paradigm should be created on federated biometric norms within UPI networks and liability treaties across national borders. Moreover, with fraudsters increasingly exploiting holistically emerging technologies as tools for ill, an adaptive and dynamic paradigm on legal and technological fusion becomes a challenge and an imperative.