Indexed with SJIF
Impact Factor: 4.471
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
A Peer-Reviewed Refereed Online Law Journal

ARTIFICIAL INTELLIGENCE AND CYBER CRIMES IN THE FINTECH INDUSTRY – A DOUBLE-EDGED TOOL

Ms. Deepa Manickam[1], Prof. (Dr.) S. Amirthalingam[2], Ms. AR. Anusri[3]
[1]Research Scholar and Assistant Professor of Law, [2]Professor of Law, Tamil Nadu National Law University, Tiruchirappalli
[3]LL.M Business Law, Advocate, Karaikudi
deepamanickam@tnnlu.ac.in, amirtham@tnnlu.ac.in, anusriar97@gmail.com

Abstract--

"Banks should remain vigilant enough to protect their customers"

- State Bank of India (SBI) vs Pallabh Bhowmick and Ors.

The S.R. Mittal Working Group, constituted by the RBI in 2001, introduced the first 'Internet banking guideline' paving the path to introduce Information Technology (IT) in the banking sector. Contemporary technological advancements in digital financial services proves to be a boon for the fintech industry and reduced risks in financial transactions in daily life. The International Data Corporation Report [2022-2026] states that banking and retail are the two largest AI investors. The financial well-being of each bank customer gets affected and exposes to cybercrime or Online Financial Frauds (OFFs), including phishing, ransomware, money mules, and deepfakes. Social engineering attacks use Artificial Intelligence (AI) and Machine Learning (ML) to target customers through synthetic media. The AI-influenced cybercrimes include voice emulation and synthetic voice/text generations to gain unauthorized access to bank accounts. Interestingly, the RBI Annual Report 2023-2024 explores the possibilities of AI in risk management including an AI-based money mule hunter to protect the privacy and financial stability of individuals. The EU AI Act has made it possible to categorize AI risks. India's IT legal framework, the IT Act 2000 and the Digital Personal Data Protection Act 2023, should be made more adaptable to the fast-changing technological and economic landscapes.

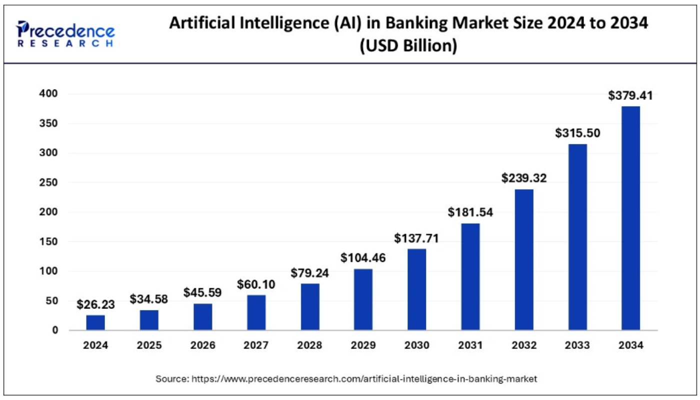
Keywords: Cyber Crimes- Artificial Intelligence (AI)- Fintech- Risks- Cyber security infrastructure.

INTRODUCTION

Financial services show no signs of slowing down since it has progressed with the integration of artificial intelligence (AI) and machine learning (ML) to distributed ledger technology (DLT). The said advancements don't stop with transformation but reshapes the future of finance. India's FinTech ecosystem is at the forefront of global transformation. The FinTech sector is expected to rise from USD 110 billion to USD 420 billion over the next five years, achieving compound annual growth rate (CAGR) of 31%. India has remarkable initiatives including UPI, JAM Trinity and ULI in the Digital Public Infrastructure to achieve economic growth.

AI AND CYBER CRIMES IN FINTECH INDUSTRY

India's fintech industry is a story of vision, resilience and adaptability.[1] Fintech entities are prone to risks of cybercrimes or online financial frauds apart from operational resilience, operational risks and data governance etc. Focus should be laid on illegal money flowing through the financial system worth USD 3 trillion in 2023 fuelling the drug trafficking, human trafficking and terrorism. Particularly, in India, 1750 crores were siphoned off during the first few months of 2024 in online financial frauds. Cyber criminals adopt new AI technologies to commit deep fake voice and text synthetic identity frauds, money mule accounts, ransomware frauds, phishing against the online banking infrastructure. Here is a stat for AI in banking market,



Source: https://www.precedenceresearch.com/artificial-intelligence-in-banking-market

CYBER CRIMES IN FINTECH INDUSTRY

- AUTOMATED PHISHING ATTACKS

Phishing tools backed by artificial intelligence may create tailored emails and messages that seem like they came from reputable banks.Scammers can utilize Natural Language Processing (NLP) to create communications that sound legitimate in order to fool users into divulging crucial information.

- DEEPFAKE FRAUD & SYNTHETIC IDENTITY THEFT

Bank employees, CEOs, and even consumers may be fooled by using deepfake audios, videos and voice cloning created by artificial intelligence. In order to evade Know Your Customer (KYC) verification, cybercriminals combine actual and fraudulent personal data to construct synthetic identities and fool the bank consumers to obtain the credentials and eventually to make them lose money.

- AI-DRIVEN FRAUDULENT TRANSACTIONS

In order to evade fraud detection systems, cybercriminals employ AI to study patterns of transactions and imitate real consumer actions. With the use of machine learning (ML) algorithms, fraudsters may create bogus transactions that seem real. Bots driven by artificial intelligence can quickly try hundreds of possible login combinations (credential stuffing).

- BYPASSING ANTI-FRAUD SYSTEMS

Cybercriminals research financial institutions' fraud detection methods use AI and modify their assaults appropriately. AI models examine previous reactions to fraud detection in order to improve attack tactics and gain profit.

- RANSOMWARE-AS-A-SERVICE (RAAS)

High-value fintech targets can be automatically identified and targeted by ransomware that is augmented with artificial intelligence. Ransom demands can be optimized using AI by taking into account a company's financial condition.

- MONEY LAUNDERING USING AI & CRYPTO

AI improves ‘smurfing’ methods, where huge sums of money are divided into smaller, less suspicious transactions. AI-powered tools aid criminals in structuring transactions to evade detection by AML (Anti-Money Laundering) systems. Banks use Anti Money Laundering (AML) tools to protect their customers.

- MONEY MULE

Money mule individuals receive illegal money in their account from an unknown cyber criminal or third parties and transfer the same to another account. Transactions linked to money mules are frauds such as malware attacks, phishing, credit card and other related scams. Recently, RBI introduced AI money mule hunter to mitigate money mule frauds.[2]

LEGISLATIVE FRAMEWORK ANALYSIS

Various payment systems, including UPI and RuPay, are overseen by the *Reserve Bank of India (RBI)* via the *Payment and Settlement Systems Act of 2007* (PSS Act).[3] The master directions on Electronic Trading Platforms (ETP) and the Payment aggregators and Payment Gateways (PAPG) Guidelines laid out the rules for the opening and operation of accounts and the settlement of payments for electronic payments involving intermediaries[4] . As was rightly stated in the case of *Vijay Kumar Gupta v. Reserve Bank of India & Ors*.[5]that the banking system is the backbone if the Indian economy and additionally the judiciary has taken measure to protect consumer from their online financial frauds in the case of *Jaiprakash Kulkarni & Anr. Vs. Banking Ombudsman & Ors.* [6] and held robust security measures and the protection of consumers in the digital banking ecosystems. In the case of *Internet and Mobile Association of India v. Reserve Bank of India*[7] the Hon'ble Supreme Court of India invalidated the RBI Circular, therefore removing the ban on trading cryptocurrencies in the country. While invalidating the RBI Circular, the Hon'ble Court ruled that the central bank could regulate or prohibit "anything" that could affect India's financial system, regardless of whether it was part of the credit or payment systems.[8] *The Master Direction on Issuance and Operation of Prepaid Payment Instruments,* more often known as the PPI Guidelines, is in charge of regulating prepaid instruments like e-wallets. Innovative financial products can be tested in a controlled environment with the support of the Reserve Bank of India's sandbox system for the fintech industry.[9] Under the *Securities and Exchange Board of India Act 1992* and *the Securities Contracts Regulation Act 1956,* the SEBI has the power to oversee the securities markets and the people involved in them. In India, the SEBI (Alternative Investment Funds) laws, 2012 govern the use of AIFs in Fintech and spell out the procedures for registration and investor protection.[10] These laws pertain to hedge funds in particular. *The Companies Act, 2013* requires fintech businesses to register and conform with industry laws; another important regulation is the NPCI Regulations, which control payment systems like UPI and RuPay.[11].*Information Technology Act,2000* and the Digital Personal Data Protection Act 2023 (DPDP)[12] govern data protection, cyber security and online transactions in India. Companies might face legal consequences under the DPDP Act if they do not adequately safeguard their customers' sensitive personal information. Breach of a legally binding contract by disclosure of confidential information is punishable under Section 72A.[13]

SUGGESTIONS TO ENHANCE CYBER SECURITY INFRASTRUCTURE

Despite the many advantages that AI may bring to cybersecurity, there are still obstacles to overcome and it can be cured through the suggestions.

DATA PRIVACY AND ETHICS

Privacy and ethics are major issues with artificial intelligence (AI) in cybersecurity. To safeguard sensitive information and stay in compliance with rules, financial institutions must guarantee that AI systems are sturdy. EU AI Act 2024 can prove as a pioneer in assisting with the AI systems analysis.

The G7 Hiroshima AI Process-2023 introduced key pointers, including those in ethical AI development, and the need for transparency and accountability in AI deployment.[14]

REAL-TIME FRAUD RISK MONITORING AND MANAGEMENT (FRM)

AI money mule hunter and Anti Money Laundering software are being used in fighting against the contemporary online financial frauds. The Indian Cyber Crime Coordination Centre (I4C), plays a crucial role in fortifying defenses against these threats. In essence, it is high time to embrace new technologies to strengthen the cyber security infrastructure but at the same time awareness and education should also be made among all stakeholders to protect the integrity of the system.

EVOLVING THREAT LANDSCAPE AND NEED FOR SELF- REGULATION

While AI programming introduces a ‘black box’ algorithm, it lacks transparency in automated decision-making. This unpredicted training of the AI tools makes it destructive for a greater number of cybercrime outcomes, including data breaches and require ethical practices. Financial institutions must be vigilant in their defense against cyberattacks since these threats are dynamic and ever-changing. To successfully tackle new threats, AI systems need to be updated and polished on a regular basis.[15] the industries-led bodies may set standards, promote best practices, and monitor compliance to act as a bridge between FinTech entities, regulators, and consumers in the digital banking ecosystem.

INTERNATIONAL COOPERATION

The Mutual Legal Assistance Treaties (MLATs) are required at the level of regulators across countries to regulate the borderless online financial frauds. harmonized frameworks are crucial to address the growing challenges related to risks in data privacy, cyber security and financial integrity. Adoption of technical standards globally will prove to be a sound argument in strengthening the cyber security infrastructure.

CONCLUSION

As a whole, it is better to understand AI as a double-edged tool which offer enhanced cyber security, detects significant online frauds enabling sophisticated cyber crimes in the fintech industry across the world. In India, specifically, RBI and various other leading banks started working with AI to mitigate frauds to enhance privacy and financial well-being of their customers. AI- driven algorithms help detect anomalies, automate compliance, and protect sensitive data. Nevertheless, cyber criminals efficiently use AI to perform the above-mentioned attacks with automated hacking tools. The fast evolution of AI demands persistent adaptation of cyber security measures, ethical AI governance by the fintech industries, and regulatory mechanisms. While AI enhances fintech’s resilience, it also poses unprecedented threats. Striking a balance between innovation and security is crucial to ensure AI remains a force for good in financial services.

REFERENCES

[1] “Special-Keynote-Address-delivered-by-Shri-Ajay-Kumar-Choudhary-Non-Executive-Chairman-and-Independent-Director-NPCI-Aug-29-2024-5th-Global-Fintech-Fest-Mumbai.pdf.”

[2] S. N. Kundu Rhik, “RBI to introduce real-time AI-driven systems to check cyber fraud,” mint. Accessed: Feb. 04, 2025. [Online]. Available: https://www.livemint.com/industry/banking/rbi-ai-driven-systems-cyber-fraud-digital-transactions-warning-system-11730111591129.html

[3] “Reserve Bank of India.” Accessed: Feb. 05, 2025. [Online]. Available: https://www.rbi.org.in/commonman/english/scripts/FAQs.aspx?Id=420

[4] admin, "Fintech Laws In India: Understanding The Regulatory Regime," Corridalegal. Accessed: Feb. 05, 2025. [Online]. Available: https://corridalegal.com/fintech-laws-in-india-understanding-the-regulatory-regime/

[5] *Vijay Kumar Gupta v. Reserve Bank of India & Ors. (Neutral Citation: 2022/DHC/005031)*. Accessed: Dec. 31, 2024. [Online]. Available: https://www.verdictum.in/pdf_upload/cds21112022cw54532008165116watermark-1440456.pdf

[6] J. Kulkarni, *Jaiprakash Kulkarni & Anr. Vs. Banking Ombudsman & Ors. WRIT PETITION NO.1150 OF 2023-MARCH 2024*.

[7] "Internet And Mobile Association Of ... vs Reserve Bank Of India on 4 March, 2020." Accessed: Feb. 05, 2025. [Online]. Available: https://indiankanoon.org/doc/12397485/

[8] A. Hayes, "A whole new cryptocurrency world: Supreme Court of India lifts RBI ban," Twenty Essex. Accessed: Feb. 05, 2025. [Online]. Available: https://www.twentyessex.com/a-whole-new-cryptocurrency-world-supreme-court-of-india-lifts-rbi-ban/

[9] A. Verma, "All you need to know about FinTech Law in India," iPleaders. Accessed: Feb. 05, 2025. [Online]. Available: https://blog.ipleaders.in/need-know-about-fintech-law-india/

[10] Accessed: Feb. 05, 2025. [Online]. Available: https://www.sebi.gov.in/acts/act15ac.html

[11] "CompaniesAct2013.pdf." Accessed: Feb. 05, 2025. [Online]. Available: https://www.mca.gov.in/Ministry/pdf/CompaniesAct2013.pdf

[12] *Digital Personal Data Protection Act, 2023*.

[13] V. Kapoor, "Fintech and changing financial industry in India," iPleaders. Accessed: Feb. 05, 2025. [Online]. Available: https://blog.ipleaders.in/fintech-and-changing-financial-industry-in-india/

[14] OECD, *G7 Hiroshima Process on Generative Artificial Intelligence (AI): Towards a G7 Common Understanding on Generative AI*. OECD Publishing, 2023. doi: 10.1787/bf3c0c60-en.

[15] T. Krakowczyk, "The Role of AI and Cybersecurity in the Financial Sector," Software Mind. Accessed: Feb. 05, 2025. [Online]. Available: https://softwaremind.com/blog/the-role-of-ai-and-cybersecurity-in-the-financial-sector/