



Digital Frauds: The Rise of AI-Enabled Banking Frauds in India

Bhatt Ishita Rajeshbhai
Research Scholar,
Department of Commerce,
Krantiguru Shyamji Krishna Verma Kachchh University
<https://doi.org/10.5281/zenodo.20488799>

Abstract

The development of Artificial Intelligence (AI) has created a double effect in the banking sector. While it supports the detection of fraud and cybersecurity applications, it also delivers advanced tools for cybercriminals to carry out advanced financial frauds. Techniques such as fake identities, phishing, Ransomware, Malware, Trojan horses are the most common attacks nowadays. With the increasing use of online banking, mobile payments, and digital financial service platforms, the number of cyber-supported banking frauds has increased internationally. This paper examines the increasing trend of banking frauds in the era of artificial intelligence, analyses the increasing cybersecurity challenges, and discovers technological strategies to make strong financial security. This study highlights the need for innovative cybersecurity frameworks and collaboration between financial service institutions and technology providers to efficiently fight AI-supported financial crimes.

Keywords: Artificial Intelligence, cybersecurity, financial frauds, Malware, phishing

Introduction

The increasing trend of banking frauds requires a complete understanding of how artificial intelligence (AI) can help to detect cyber criminals and it also poses a threat of hacking. The banking sector has suffered a major revolution due to technological advancements, digital banking services, and the extensive adoption of artificial intelligence (AI). Financial institutions progressively depend on digital platforms, online banking systems, and mobile payment applications to provide the best services to their customers. These technological expansions have developed operational effectiveness and customer experience. The increasing use of digital financial services has made the banking industry a primary target of cybercriminals because of weak security and weak technological infrastructure. Additionally, the increasing number of cyber fraud and online scam cases in the banking sector shows the urgent need to collaborate with strong cybersecurity institutions, AI-



driven detection systems, multi-factor authentication, and strict regulatory agreement. Financial institutions must take important steps for support cybersecurity infrastructure and improving awareness among customers and build trust towards banks.

Literature Review

Kshitij Shukla, Mohd Sajid, Akil Hussain (2025) Cybersecurity is dangerous for protect sensitive financial information and supporting user self-confidence. Main objective of the study is to study the use of machine learning in real-time risk exploration and irregularity in identification. Irregularity detection, Behavioural Analytics, Deep learning for Fraud Prevention, Real-Time Threat Detection techniques are essential for stopping financial fraud. The results of this empirical study provide strong proof of the usefulness of AI driven cybersecurity in online banking, mainly in enhancing fraud detection and risk modification.

Vishal Dineshkumar Soni (2019) the research paper explains about implementation of AI in the banking sector to diminish cyberattacks. 70% of CEOs of the capital market and banks consider cyber security a danger to their development. Few cyber-attacks directly influence on enterprise systems such as phishing. This kind of attack is hard to detect, to diminish this problem AI software tries to detect the pattern for all user accounts or devices. Author also highlighted about Robo -advisor. Main advantage of the using AI is it helps to handle the risk calculation process easily and important data of customers is analysed by AI technologies.

Oluwatoyin Ajoke Farayola (2024) Traditional security methods are no longer acceptable to fighting sophisticated attacks, requiring innovative solutions. The combination of AI, Blockchain technology, and BI (Business Intelligence) denotes a significant shift from responsive to proactive security actions. Identity theft denotes another pressing concern inside the banking sector. Author concludes that by acceptance upgraded technologies and adopting proactive security measures, banks can protect their systems, protect customer assets, and maintain trust in digital world.

Raju Kumar, Surya Kiran, Arjun (2025) In 2023, international financial losses due to cybercrime beat \$12 billion, with banking-related accounting for nearly 40% of that figure, according to the International Monetary Fund (IMF). Artificial intelligence offers a transformative pathway advancing, mainly through unofficial learning techniques that detect irregularities without the support of datasets. Main objective of the study is to bridge gaps by suggesting an AI driven background to detect unsupervised banking cybersecurity fraud. Unsupervised learning algorithms method the core of the detection system. Quantitative results from historical data testing disclosed a precision of 87%, a recall of 82%, and an F1-score of 84%, outperforming traditional rule-based systems by 15–20% across these metrics.



Tamanna Choithani, Asmita Chowdhury, Shriya Patel, Poojan Patel, Daxal Patel, Manan Shah (2022)

Today AI is a leading sector for research in different fields such as Transportation, Security Investigation, Engineering, education, medical, business, accounting, finance, marketing, economics, stock market, Agriculture, Sports etc. The Internet can be defined as a transmission network that connects individuals to data. AI not only authorizes banks by industrializing their knowledge workforce, but it also makes the whole automation process smart enough to address competition and cyber risks. Author also highlighted AI gains an enhanced understanding of customers and behaviours based on past communication.

Priyanka Chadha, Sonali P. Banerjee, Arhita Uppal, Kanika Rana (2024)

E-banking in India is not a very old term in India. It is just started in India in late 90's before the only Branch banking system was established. In India the Internet banking was first launched by ICICI bank. Additionally HDFC and Citibank followed with E-Banking services in year 1999. Public WIFI also give opportunity to hackers. Main objective of the study is to evaluate whether there is different in awareness of the users on the basis of Age and Gender. Author found that, around 50% of the respondents aware about the most common cybercrimes such as Phishing, malware-based attack, false websites, and public Wi-F.

Kalikant Mishra, M. Khalid Azam, S.O.Junare (2020)

study about Role of Forensic Audit in Controlling Financial Statement Fraud: A case study of Satyam Computers. Study is based on secondary data which is collected from SEBI, Satyam Company, investigative agencies like CBI, State Crime Branch of Andhra Pradesh, Ministry of Finance, Govt. of India, and RBI etc. Author highlighted case study of satyam Computers Ltd. The membership of two Partner's partnership was cancelled by ICAI and they settled their US court case after making payment of \$25.5 million to Satyam investors.

Tirumalaraju Naveen, G.V.Satya Sekhar (2024)

As per the RBI reports, Indian banks have stated 3,67,845 fraud cases amounting to nearly Rs.5.74 lakh crores, out of which, Rs.75,912 crores fraud amount is from eight individual commercial accounts. Author deeply study about eight top commercial fraud cases in the banking sector.

Research gaps

- Limited studies on the integration of AI with cybersecurity systems in banks.
- Limited research on privacy challenges of AI in banking security.
- Few studies have discussed about the case studies of banking frauds.



Objective

- To examine the increasing banking frauds in the digital banking era.
- To analyse the role of artificial intelligence in helping and detecting banking frauds.
- To identify the major types of cyber frauds that affecting in the banking sector.
- To suggest strategies and technological solutions to reduce banking frauds in the era of artificial intelligence.

Research Methodology

This research uses an exploratory research methodology to understand why banking frauds have been increasing nowadays and examine the role of cybersecurity and AI in reducing these frauds by analysing the literature reviews and case studies.

What is banking fraud?

Bank fraud is the use of potentially illegal means to obtain money, assets, or other property owned or held by a financial institution, or to obtain money from depositors by fraudulently posing as a bank or other financial institution. In many instances, bank fraud is a criminal offence.

Types of Banking Frauds

- **Fraud through UPI:** In this scam payment links are sent by fraudsters through an SMS. These payment links look similar to original payment gateway. After clicking on these links users are directed to the UPI payment application installed on the phone where upon giving permission by entering their UPI PIN the amount is debited from their bank account immediately.
- **Fraud through Telecallers & KYC:** Hackers established panic in the victims mind, and they ask for sensitive bank details such as, full account number, ATM card details, OTP, PIN. Sometimes they call victim and say your account has been blocked because of you don't do KYC. And victims give their details easily.
- **Wire transfer fraud through Emails:** sometimes hackers sent notification such as, you have won ₹5000000! Please click the given link and claim all of it!
- **Account Takeover:** cybercriminals gain unauthorised access to a customer's account, regularly to important financial transactions. Phishing, credential Stuffing, Social Engineering are the example of popular cyber frauds.
- **Identity theft:** phishing attempts seek to steal information of credit card, ATM PIN, passwords in order to take over social network data or access the victim's bank account details.



- **Trojan virus:** Trojan Horses is a malicious programme that, in contrast to other virus, spreads quickly instead of replacing itself. By opening the attachments in spam email, user can activate this type of virus.
- **Ransom Ware:** this type of attacks is proposed to avoid access to a computer or collection of computers unless a certain amount of money is paid. They threaten to reveal private information until the attackers receive payment.
- **Chit Fund Scams:** Unprofessional conduct or misuse of funds in collective investment schemes like the Saradha scam.
- **Ponzi Schemes:** Promises of high returns through fake investment schemes.

Top banking frauds in India

As time passes, many methods and approaches have been used to commit bank fraud in India. Here are some case studies mentioned below.

Punjab and Maharashtra Co-operative (PMC) Bank Scam (2019)

Amount: 6500 crore

When it was exposed that bank employees had secret non-performing assets worth more than 6,500 crore in collaboration with the promoters of the “Housing Development and Infrastructure Limited (HDIL)”, the PMC Bank fraud came to light. Failure to right to use their own money resulted in depositors being in a dilemma.

Bank of Baroda Forex Scam (2015)

Amount: 6000 crore

Scam: Illegal forex transactions and remittances to foreign accounts.

Unfamiliar transfers computation almost ₹6,000 crore were made from the Bank of Baroda's Ashok Vihar branch in Delhi to a number of organisations in Hong Kong. Here, fake accounts were used to conduct illicit business.

Nirav Modi-PNB Scam (2018)

Amount: ₹11,400 crore

Scam: Fake Letters of Undertaking (LoUs) issued by PNB officials were misused to secure unauthorized loans.



The scam controlled to a massive loss of capital and goodwill for PNB, highlighting the fact that India's banking sector is not immune from insider fraud. The case also highlighted the importance of better supervision and monitoring in public sector banks.

Vijay Mallya-Kingfisher Airlines Debacle

Amount: ₹9,000 crore

Scam: Loans for operational purposes were distracted to personal ventures.

Kingfisher Airlines' owner, Vijay Mallya, can be called the face of financial default in the country. Umesh Reddy's airline used more than ₹9,000 crores from various banks and has been unable to return this due to operational inefficiency and alleged monetary management fraud.

Saradha Chit Fund Scam

Amount: ₹2,500 crore

Scam: A Ponzi scheme promising high returns through fraudulent investment schemes.

Saradha Group is involved in the biggest Ponzi scheme in India, which swindled money from poor investors in western West Bengal and Assam. Who stuck a catch so deep into the innocent public that it cheated over ₹2,500 crores from small investors promising high returns on chit fund investments and real estate business.

Saradha's case emphasized the need for strict rules to safeguard ordinary people's money and check financial market fraud.

Rotomac Pens Fraud

Amount: ₹3,695 crore

Modus Operandi: Loans planned for business development were tapped for personal use.

Among the fraudsters, one of the most notorious is Vikram Kothari, a Rotomac Pens fraudster who had embezzled ₹3,695 crore borrowed from different public sector banks. In the case, it pointed out that the banks were exposed to fake activities due to borrowers manipulating existing defects in the system. After the fraud, Kothari and his family received a legal outcome, and the banks were blamed for poor risk evaluation. Sprouse said the experience supported renewed efforts to increase understanding and regulation about multi-bank lending.



Sahara India Scam

Amount: ₹25,000 crore

Scam: Mismanagement of collective investment scam, leading to investor losses.

The Sahara India Scam was misusing the money collected through optionally fully convertible debentures (OFCDs). More than ₹25,000 crore was collected from ordinary investors in the name of investment plans and products, which went against SEBI rules.

ICICI Bank-Videocon Loan Case

Amount: ₹3,250 crore

Modus Operandi: Alleged quid pro quo in loans sanctioned by ICICI Bank to Videocon Group.

Earlier, former CEO and MD Chanda Kochhar faced allegations of providing favours to Videocon Group for personal gratification. These issues are best illustrated in the case of governance failures and ethical leadership at the centre of these financial institutions.

These cases show the variety of frauds that occur in India, from loan defaults and money theft to financial record manipulation and the use of false documentation. They draw attention to the necessity of more stringent regulatory oversight and enforcement, as well as better risk assessment and lending procedures within the banking industry, to stop such tragedies.

What is cybersecurity?

Cybersecurity is the combination of methods, processes, tools, and behaviours that protect computer systems, networks, and data from cyberattacks and unlawful access. Although extremely rooted in technology, the efficiency of cybersecurity also very much depends on people.

Why Cybersecurity is Important in Banking?

Cybersecurity is important in protection of financial institutions against the powerful strategies by cybercriminals, ensuring the protection of sensitive customer data and maintaining trust in the banking system.

- Cybersecurity protects sensitive bank details such as account details, transaction history, and personal data from unofficial access.
- It helps to avoid cyber threats like phishing, malware, ransom ware, and identity theft in digital banking systems.



- It provides security for online transactions and mobile banking services for customers.
- Cybersecurity helps banks to build trust among customers.
- A strong cybersecurity structure helps banks observe with regulatory standards issued by the Reserve Bank of India and other authorities.
- Cybersecurity helps to maintain stability of the banking system in a digital economy.
- Cybersecurity not only cares for personal data, but also ensure the safety and dependability of services that support millions of users daily.

Role of Artificial Intelligence in Banking

- Artificial Intelligence helps banks automate routine operations and improve efficiency in financial services (McKinsey & Company, 2021).
- AI enables banks to detect dishonest transactions quickly by analysing large volumes of financial data.
- AI-powered chatbots expand customer service by providing 24/7 support to banking customers and this strategy helps to increase customer satisfaction.
- AI strengthens cybersecurity systems by detecting suspicious activities in real time.
- AI improves credit scoring and loan approval processes by analysing customer financial behaviour (World Bank, 2020).
- AI enables personalized banking services based on customer preferences and transaction patterns.
- AI decreases operational costs by automating repetitive banking tasks and processes.
- Artificial Intelligence enhances overall banking security, efficiency, and innovation in the digital economy (Reserve Bank of India, 2022).

Why AI is important in Banking Sector?

With the help of AI customers improve their decision-making about financial matters. They are more likely to stay with banks that use critical-power AI technology to helps them for managing their money effectively.

Challenges of implementing AI and cybersecurity

- Lack of transparency.
- Cybercriminals are being smarter day by day. They know how to attack AI models directly.
- Traditional firewalls are not enough. Banks need to construct security into the AI lifecycle from the ground up.
- Inadequate knowledge among the general population.



Conclusion

Artificial intelligence and cybersecurity are widely used in banks and financial institutions. This paper concludes that artificial intelligence is known as a concept to copy human brains. AI helps to improve customer relations and experience, enhance the efficiency of banking processes, and develop security and risk management. The importance and challenges in implement of AI and cybersecurity in the banking sector is also discussed in this paper. The paper also study about some major banking frauds. Information About cyberattacks and the cost of solutions is provided by AI towards banks and financial institutions. Various issues related to fraud and data breach are identified by artificial intelligence techniques. The integration of AI and cybersecurity plays an essential role in protecting banks and financial institutions from increasing banking frauds.

References

- Soni, V. D. (2019). Role of artificial intelligence in combating cyber threats in banking. *International Engineering Journal For Research & Development*, 4(1), 7-7.
- Farayola, O. A. (2024). Revolutionizing banking security: integrating artificial intelligence, blockchain, and business intelligence for enhanced cybersecurity. *Finance & Accounting Research Journal*, 6(4), 501-514.
- Shukla, K., Sajid, M., & Hussain, A. (2025). AI-Driven Cybersecurity in Online Banking: Enhancing Fraud Detection and Risk Mitigation. *Asian Journal of Business Research & Innovation (AJBRI)*, 1(2).
- Kumar, R., & Kiran, S. (2025). AI-Driven Frameworks for Unsupervised Fraud Detection in Banking Cybersecurity. *Int. J. Sci. Eng. Appl*, 14(3), 1-5.
- Choithani, T., Chowdhury, A., Patel, S., Patel, P., Patel, D., & Shah, M. (2024). A comprehensive study of artificial intelligence and cybersecurity on bitcoin, crypto currency and banking system. *Annals of Data Science*, 11(1), 103-135.
- Chadha, P., Banerjee, S. P., Uppal, A., & Rana, K. (2024). Unraveling the Essence of Cybersecurity in Banking: Preserving Financial Integrity and Building Confidence. *International Journal of Business Research & Innovation*, 12, 17-29.
- Mishra, K., Azam, M. K., & Junare, S. O. (2021). Role of forensic audit in controlling financial statement fraud: a case study of Satyam computers. *Psychology and education*, 58(2), 4016-4025.
- Naveen, T., & Sekhar, G. S. (2024). Analysis of Corporate Frauds in the Indian Banking Sector. *European Economic Letters*, 14(1), 1797-1802.
- Mundhara, A. (2024). "Imapact of Cyber- Attacks on Banking Institution in India: A study of Safety Mechanism and Preventive Measure. *Shalax International Journal of Management*, 11(11), 142-148.



- Ghosh, A. (2023). REASONS FOR BANK FRAUDS AND THE IMPLEMENTATION OF PREVENTIVE SECURITY CONTROLS IN INDIAN BANKING INDUSTRY. *Indian Journal of Law and Legal Research*, 5(6), 2466-2484.
- Dharshini, K., Vishnupriya, B., L.Shariya, P., Guruharini, M. (2025). DATA PROTECTION AND CYBER SECURITY IN BANKING COMPLIANCE, BREACHES, LIABILITIES. *International Journal for Research Trends and Innovation*. a302- a309.
- Role of Cybersecurity in Online Banking (2025)
- Banks, financial institutions should safeguard security against cyber threats: RBI. (2023). *The economic Times*.
- McKinsey & Company. (2021). *Global Banking Annual Review*.
- World Bank. (2020). *Artificial Intelligence in Financial Services*
- Reserve Bank of India. (2022). *Report on Trend and Progress of Banking in India*
- https://en.wikipedia.org/wiki/Bank_fraud
- https://www.gktoday.in/rbi-cybersecurity-framework/?utm_source
- <https://www.kychub.com/blog/top-banking-frauds-in-india/>
- <https://www.fortinet.com/resources/cyberglossary/what-is-cybersecurity>
- <https://www.ibm.com/think/topics/ai-in-banking>
- <https://theintellify.com/ai-implementation-strategy-challenges/>

Certificate No.: 04072026003



**MULTIDISCIPLINARY COSMOPOLITAN JOURNAL OF RESEARCH
(MUCOJOR)-2583-9829 (On-line)**

International Peer Reviewed and Refereed Journal

CERTIFICATE OF PUBLICATION

The Board of Multidisciplinary Cosmopolitan Journal of Research
(MUCOJOR) is hereby awarding this certificate to

Bhatt Ishita Rajeshbhai

In recognition of the publication of the paper entitled

Digital Frauds: The Rise of AI-Enabled Banking Frauds in India

Published in Volume 04, Issue 07, June 2026.

EDITOR IN CHIEF