CYBER SECURITY IN THE INDIAN BANKING SECTOR: TRENDS, THREATS AND STRATEGIC RESPONSES

Dr. Meena Sharma*

Abstract

This study examines the rising incidence of cyber fraud in India's banking sector, driven by rapid digitalisation and increased adoption of electronic payment systems such as UPI and mobile banking. Using secondary data from the Reserve Bank of India (RBI), Ministry of Home Affairs (MHA) and National Cyber Crime Reporting Portal (NCRP), the study analyses recent trends in cyber fraud cases and financial losses during 2022-25. The findings indicate that while cyber fraud cases are high in volume and increased by over 70% between 2022-25, the average value per case remains relatively low, highlighting the dominance of retail digital fraud. The paper also identifies key vulnerabilities, including social engineering attacks and gaps in user awareness. It emphasises the growing role of artificial intelligence in fraud detection and prevention, while recommending policy-level, institutional and customer-centric strategies to strengthen cyber security resilience in the Indian Banking ecosystem.

Keywords

Cyber Security, Digital Banking, Cyber Fraud, UPI Fraud, Artificial Intelligence in Banking, Financial Risk Management

Introduction

The Indian banking sector has undergone a profound transformation over the past decade, driven by rapid advancements in digital technologies and proactive policy initiatives. The development of mobile banking apps, the introduction and broad use of the Unified Payments Interface (UPI) and the emergence of fintech platforms have significantly changed how financial services are provided and used. With billions of transactions performed each month, India is now one of the biggest digital payment ecosystems in the world, demonstrating improved financial inclusion, convenience and operational efficiency.

This digital shift has significantly reduced transaction costs, improved accessibility in rural and semi-urban areas and enabled real-time fund transfers. This shift has been expedited by Government programs like Digital India and the need for a cashless economy. Banks are using data analytics, cloud computing and Application Programming Interfaces (APIs) to offer seamless and customised consumer experiences. However, the financial sector is now more vulnerable to cyber threats due to rapid digitisation, which has also increased the attack surface for cybercriminals. (RBI, 2024; NPCI, 2025)

Cyber crime in India has grown in both scope and sophistication in tandem with this expansion. Complex, multi-layered attacks incorporating social engineering, malware injection, identity theft and Artificial Intelligence (AI)-driven fraud processes

*Professor (Banking and Finance), VES Business School.

have supplanted earlier kinds of cyber fraud, such as simple phishing emails and phoney lottery schemes. Cybercriminals are increasingly employing techniques like deep fake communications, impersonation schemes, fraudulent mobile applications and phoney investment platforms to take advantage of both technological flaws and human behavioural weaknesses. Malicious actors have increased the speed, accuracy and scope of these attacks by incorporating automation and artificial intelligence.

Recent data highlights the scale of cyber fraud in India, with over 36.4 lakh cases reported in 2024[1] and rising financial losses, though actual figures may be higher due to underreporting. Despite efforts by the regulators, increasing digital adoption and low user awareness continue to outpace security measures.

Cyber security has, thus, become vital to financial stability, requiring a holistic approach combining regulations, technology (Artificial Intelligence/ Machine Learning) and user awareness. This remains a gap in the integrated analysis of digital payment fraud and institutional response mechanisms.

Literature Review

Recent academic and policy literature highlights the growing systemic importance of cyber security in modern financial systems. Reserve Bank of India (RBI) emphasizes that increasing digital transactions have significantly elevated cyber risk exposure in banks, particularly within payment systems and third–party digital ecosystems (RBI, 2024). Similarly, Aldasoro, Frost, Gambacorta and Whyte (2022) identified cyber risk as a major source of financial instability due to interconnected networks, contagion effects and operational concentration risks.

Kshetri (2023) found that cyber crime in emerging economies such as India, is driven by weak digital literacy, low cyber security awareness, regulatory gaps and increasing dependence on smartphones. In the Indian context, rapid adoption of UPI, mobile wallets and app-based banking has expanded convenience but also increased fraud opportunities. Bose and Leung (2023) observed that financial institutions are increasingly deploying Artificial Intelligence (AI), Machine Learning (ML) and predictive analytics for fraud monitoring. These technologies improve anomaly detection, reduce manual intervention and enable real-time transaction screening. However, concerns remain regarding false positives, privacy issues, algorithmic bias and explainability.

In the study by Romanosky (2016) found that data breaches impose significant financial and reputational costs on financial institutions, often leading to customer attrition and regulatory penalties. This suggests that cyber security failures are not only technical risks but also strategic business risks.

Anderson et al., (2019) estimated that the global cost of cyber crime is substantially higher than previously believed when hidden economic losses, productivity decline, fraud recovery costs and trust erosion are included. Their findings support the need for stronger preventive cyber security investment rather than reactive fraud management.

Junger, Montoya and Overink (2017) highlighted that phishing attacks succeed primarily due to behavioral manipulation rather than technical sophistication. Victims often respond under urgency, fear, authority pressure or greed incentives. This is highly relevant in India, where One-Time Password (OTP) fraud, fake Know Your Customer (KYC) alerts and impersonation scams dominate retail fraud patterns.

PwC (2025) reported that social engineering frauds, phishing attacks, impersonation scams and identity theft continue to account for a dominant share of banking fraud globally. Deloitte (2026) similarly highlighted behavioral vulnerabilities such as trust bias, urgency bias, fear response, over confidence

[1]National Cyber Crime Reporting Portal.

and greed motivation as major reasons why customers fall prey to digital fraud.

Arner, Barberis and Buckley (2020) noted that fintech innovation and open banking models increase efficiency but simultaneously create new cyber security vulnerabilities through APIs, outsourced platforms and ecosystem integration. This is especially relevant in India's fast-growing digital finance environment.

NCRB (2024), MHA (2025) and RBI reports indicated that India has experienced sharp growth in UPI-related frauds, fake investment scams, SIM swap attacks and identify theft. However, existing studies often examine either aggregate cyber crime trends or global frameworks, with limited India-specific integrated analysis combining fraud patterns, behavioral economics and AI-based response system.

Thus, the literature establishes cyber security as a multidimensional issue involving technology, governance, human behavior and financial stability. Yet there remains a significant research gap in evaluating India's recent cyber fraud surge through an integrated banking sector lens.

Research Gap

Despite extensive literature on cyber security and financial risk, there is limited integrated studies focusing specifically on the recent surge in digital payment-related fraud in India. Existing studies largely analyse aggregate cyber crime trends or global frameworks, with insufficient attention to:

- The behavioural dimension of retail cyber fraud.
- The divergence between high-volume and high-value fraud patterns.
- The role of AI in the Indian Banking fraud ecosystem.

Objectives

The study aims to:

- Analyse recent trends and structural patterns of cyber frauds in India.
- Examine major types and behavioural drivers of cyber crime in digital banking.
- Evaluate the role of Artificial Intelligence (AI) in fraud detection and prevention.
- To propose policy and institutional measures to strengthen cyber security resilience.

Research Methodology

The study is exploratory and policy-oriented in nature, based on secondary data. Information has been gathered from reports released by the Ministry of Home Affairs (MHA) – NCRP databases, the Reserve Bank of India and other Governmental and institutional sources. The report captures current trends in cyber fraud and financial losses in India and covers the years from 2022 to 2025. The nature of fraud, its growth patterns and their effects on the banking industry have been investigated using analytical techniques, including trend analysis and comparative analysis. Behavioural analysis in the study is based on interpretation of reported fraud patterns, documented modus operandi and secondary evidence from regulatory and crime databases.

The study does not involve primary data collection. Trend analysis, percentage growth analysis and comparative interpretation techniques were used to identify fraud patterns and financial losses. The methodology is suitable for policy–oriented research but may not capture micro-level behavioural insights.

Discussion

Trends in Cyber Fraud in India

The trajectory of cyber fraud in India reflects a dual pattern of rapid expansion in volume and disproportionate escalation in financial impact. Cyber crime has developed into a systemic issue that affects both customers and financial institutions due to the

growing digital penetration of banking, payments and fintech platforms.

Growth in Cyber Fraud Cases

Table 1: National Cyber Fraud Trends in India (2022-2025)

Year	Reported cases (Lakhs)	Estimated loss (₹ Crore)	Growth in Cases (YoY)	Growth in Losses (YoY)	Key Insights
2022	10.29	6,204	-	-	Rapid expansion of digital fraud with growing UPI usage
2023	15.96	7,465	55.1%	20.3%	Sharp rise in complaints linked to phishing and UPI scams
2024	22.68	22,845	42.1%	206.0%	Surge in losses due to investment and impersonation frauds
2025*	28.15	22,495	24.1%	-1.5%	Cases continued rising; losses stabilised due to improved blocking systems

Source: Compiled from data published by the Ministry of Home Affairs (MHA), National Cyber Crime Reporting Portal (NCRP) and RBI reports.

*Provisional data

The data indicate sustained growth in cyber fraud complaints in India from 10.29 lakhs in 2022 to 28.15 lakh cases in 2025. While the number of incidents continued to rise, financial losses surged sharply in 2024 before stabilizing in 2025, suggesting improved fraud detection, transaction freezing and intervention systems. The trend confirms that India faces a dual challenge of rising fraud frequency and evolving high-value scams models.

A major contributor to the surge in financial losses during 2024 was the rise of fake investment and trading scams, where victims were lured through social media groups, fraudulent trading applications and promises of unusually high returns. Though lower frequency than retail payment frauds, such scams involved higher average ticket size and significantly increased total losses.

Overall, the trend shows a structural shift – cases are rising rapidly, but losses have stabilized, suggesting better real-time detection and regulatory response. However, high volumes indicate fraud is becoming more widespread, posing ongoing risks to financial stability and consumer trust.

Frauds in Banking sector in India (2022-2025)

Table 2: Frauds in Banking sector in India (2022-23 to 2025-26)

Category	2022-23	2023-2024	2024-25	2025-26 (latest available)
Total fraud cases	13,462	36,052	23,879	~5,092 (H1)
Amount involved (₹Crore)	16,502	11,261	34,771	21,515 (H1)
Card/Internet Fraud (Cases and Amount involved)	High share in volume	~80% of cases (high volume)	66.8% of cases (~70,756 cases), ₹252 crore	Declining share, ₹4 crore (H1)

Category	2022-23	2023-2024	2024-25	2025-26 (latest available)
Amount from Card/Internet Fraud (₹Crore)	277	1457	520	14
Loan-related (Advances) Fraud (Cases and Amount involved)	Major share of losses (₹15,065 crore)	4113 cases, ₹9,160 crore	7934 cases, ₹31,911 crore	₹17,501 crore (H1)
Structural Trend	Legacy fraud recognition	Retail fraud surge	High-Value concentration	Continued vigilance required

Source: Report on Trend and Progress of Banking in India (2023–24, 2024–25) and subsequent updates for FY2025–26 (H1), Reserve Bank of India.

Note: H1 is April to September

RBI fraud statistics reveal a structural shift in Indian banking fraud. Retail digital frauds such as card and internet fraud account for the majority of reported cases but involve relatively lower value. In contrast, a smaller number of loan-related and institutional frauds contribute disproportionately to total monetary losses. This suggests that Indian banks must simultaneously address mass retail cyber fraud and large-value governance-linked fraud risks. Overall, the sector faces a dual challenge - rising digital fraud volume and high-value loan fraud risk – requiring stronger cyber security and improved credit risk management.

Types of Cyber Frauds in India

Cyber fraud in India is becoming more complex, driven by rapid digitalization and evolving tactics of cybercriminals. With the rise of digital banking, fraudsters increasingly exploit vulnerabilities, especially targeting users with low cyber security awareness. Platforms like Unified Payments Interface (UPI), mobile wallets and online banking have become primary channels for such frauds. These scams are not only more frequent but also more sophisticated, combining technology with psychological manipulation.

A significant proportion of cyber frauds in India are linked to social engineering techniques such as phishing, impersonation, OTP scams and fraudulent investment schemes rather than purely technical systems intrusions (Junger, Montoya, & Overink, 2017).

Common Fraud Types

Phishing Attacks: Phishing remains a significant cyber threat in India by exploiting human trust rather than technical flaws. Scammers impersonate banks or Government entities through deceptive emails and SMS, directing users to sophisticated "cloned" websites designed to steal login credentials and financial data. Because this method is highly scalable and relies on psychological manipulation, it is exceptionally difficult to stop using security software alone.

UPI and QR Code Frauds: UPI and QR code fraud exploits the "receive money" myth, where scammers trick victims into scanning codes or approving "collect requests" that authorise debits. Because UPI transfers are instantaneous and irreversible, funds are moved immediately, making recovery extremely difficult. This psychological manipulation has made UPI scams a dominant and high-impact category of modern cyber crime.

OTP/Account Takeover Frauds: These frauds use

malware, SIM swapping or social engineering to obtain One-Time Passwords (OTPs). After gaining access, they take over bank accounts and carry out illicit operations. These frauds highlight vulnerabilities in authentication systems and demonstrate how multifactor authentication can fail if users are manipulated into sharing credentials.

Investment and Trading Scams: Fake trading apps and crypto schemes are the most financially damaging frauds, where fraudsters lure victims with the promise of high returns via WhatsApp groups, mobile apps or fake trading platforms. Victims are shown fake profits to build trust before losing large sums. Though fewer in numbers, these scams account for a disproportionately high share of total losses.

Identity Theft and KYC Frauds: Cybercriminals misuse personal information such as Aadhaar card, PAN details or bank credentials to open fraudulent accounts, obtain loans or conduct illegal transactions. Identity theft is becoming a bigger worry due to the rising availability of personal information online, especially in situations involving data breaches and unprotected databases.

Impersonation and Digital Arrest Scams: In these situations, scammers pose as Government, bank or law enforcement officials and threaten victims with legal action to coerce them to provide money. These scams are especially successful with less knowledgeable consumers because they mainly focus on fear and hurry.

Malware and Fake Application Frauds: Malicious mobile apps that pose as banking or utility apps are distributed by fraudsters. Sensitive information, such as SMS, OTPs and banking passwords, can be accessed by these apps once they are installed. With malware enabling remote control and user activity monitoring, mobile devices have become a key target due to the increase in smartphone usage.

Most cyber-attacks are hybrid, combining technology with psychological manipulation and are low-cost, scalable and global in reach. This makes cyber crime in India increasingly widespread, exploiting both technological vulnerabilities and human behavior.

Investment–related Frauds: Emerging High-Value Risk

Investment–related cyber fraud has emerged as one of the fastest growing and most financially damaging categories of cyber crime in India. According to data released by the Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs, stock trading scams accounted for the highest cyber fraud losses in India during the first nine months of 2024, amounting to ₹4,636 crore across 2,28,094 complaints, highlighting the growing severity of investment-linked digital frauds. In addition, investment-related scams caused losses of ₹3,216 crore from 1,00,360 reported complaints (The wire staff, 2024, November 27). These figures indicate the rapid rise of high-value digital investment frauds in India. Fraudsters typically lure victims through social media advertisements, WhatsApp/Telegram groups, fake stock advisory services and fraudulent trading applications promising unusually high returns.

Unlike low-value phishing or OTP frauds, investment scams usually involve repeated transfers and larger ticket size, causing severe household financial losses. Victims are often shown fake dashboards displaying profits to build trust before being persuaded to invest additional funds. This indicates a structural shift in Indian Cyber fraud from high-volume retail frauds toward fewer but higher-value financially sophisticated scams.

The growing incidence of such frauds highlights the urgent need for stronger investor awareness, platform verification mechanisms, tighter digital advertising controls and coordinated enforcement between banks, regulators and cyber crime agencies.

Table 3: Indicative Share of Investment fraud in India (2024)

Category	Estimated Loss (₹ Crore)	Risk Nature
OTP/UPI frauds	Lower per case	High volume
Phishing frauds	Moderate	Mass retail
Stock trading scams	4,636+	High value
Investment – related scams	3,216	High value
Impersonation frauds	High	Psychological

Source: Indian Cyber Crime Coordination Centre (I4C), 2024; Cyber fraud complaint and financial loss statistics (January-September, 2024) and Ministry of Home Affairs, Government of India.

The table indicates that investment-related cyber frauds, though fewer in number compared to OTP and UPI scams, account for disproportionately high financial losses, making them one of the most serious emerging threats in India's digital economy. In contrast, UPI and phishing frauds are higher in frequency but generally involve lower average transaction values. This highlights a dual fraud pattern in India – mass retail frauds by volume and investment scams by monetary impact.

Behavioural Drivers of Cyber crime in Digital Banking

The rapid growth of cyber fraud in India's digital banking ecosystem is not driven solely by technological vulnerabilities but also by behavioural factors influencing customer decision-making. Fraudsters increasingly exploit cognitive biases, emotional reactions and gaps in financial literacy to manipulate users into voluntarily authorizing transactions or disclosing credentials.

Trust Bias: Many victims believe messages appearing to come from banks, RBI, police authorities or known brands. Fraudsters use official logos, caller ID masking and professional language to create legitimacy.

Urgency and Fear Appeals: Messages such as "Your account will be blocked", "KYC expired" or "Police action initiated" create panic, leading users to act quickly without verification.

Greed and Reward Motivation: Fake investment schemes, cashback offers, lottery winnings and job scams exploit the desire for quick financial gains.

Convenience Behaviour: Users often approve UPI requests, click links or share OTPs quickly to save time, especially during busy hours.

Low Digital Literacy: First-time digital users, elderly citizens and rural customer may lack awareness regarding QR codes, collect requests, fake apps and phishing links.

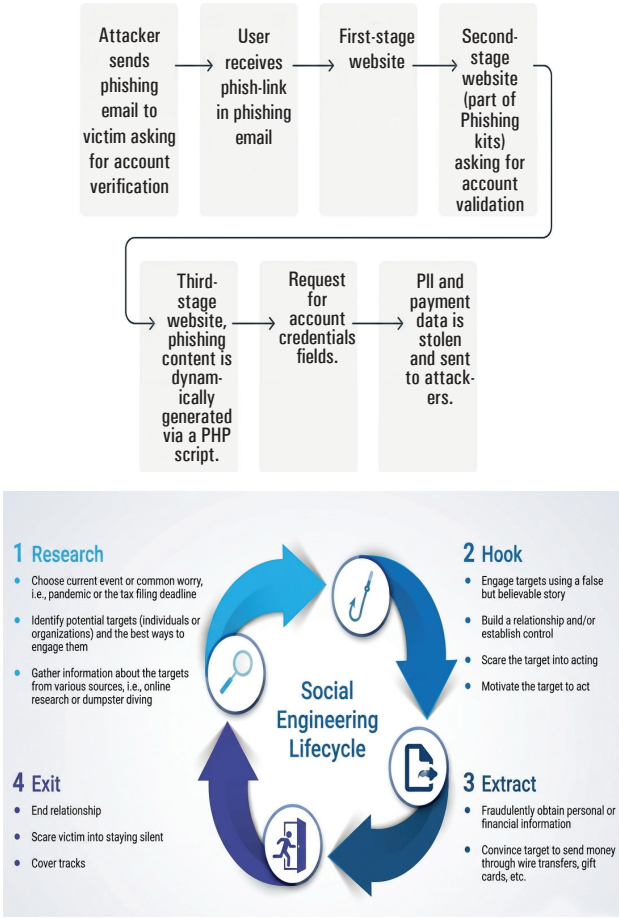
Overconfidence Bias: Experienced smartphone users may underestimate cyber risk, assuming fraud only happens to others.

These behavioural factors indicate that cyber fraud prevention requires not only stronger technology but also behavioural interventions such as warning prompts, friction-based authentication, customer education and simplified fraud alerts.

Modus Operandi of Cybercriminals

Cyber fraud in India has evolved into a multi–stage, tech-driven and behaviour-based process, where criminals use integrated tactics like malware, social engineering, data analytics and financial laundering. Despite variations, most cyber crimes follow a predictable lifecycle, as observed in the Ministry of Home Affairs (MHA) and the National Crime Records Bureau (NCRB) data.

Figure 1: Life Cycle of Cyber Fraud in India



Source: Compiled by Author

Figure 1 highlights the sequential lifecycle of cyber-fraud, emphasizing critical intervention points.

Stages of Cyber Fraud Life Cycle

***Target Identification and Data Collection*:** Cybercriminals collect personal and financial data from sources like the dark web, phishing lists, hacked databases and social media. Growing digital footprints and low awareness, especially among first-time users, make individuals more vulnerable to targeted attacks (NCRB).

***Social Engineering and Initial Contact*:** Fraudsters use messaging apps like WhatsApp, emails, SMS and phone calls, posing as banks or authorities and using urgency, fear or lucrative offers to manipulate them. Around 70-80% of cyber frauds involve social engineering, making human behaviour the key vulnerability.

***Credential Theft/Compromise*:** After gaining trust, fraudsters trick victims into sharing PINs or OTPs, clicking on malicious links or installing fake apps, often aided by malware. The RBI highlights that such credential breaches are the main cause of digital banking fraud, especially in card and online transactions.

***Transaction Execution*:** Once access is gained, scammers execute quick transactions via UPI, cards or online banking, often in multiple small amounts to avoid detection. Though low in value, such digital frauds account for over 66% of banking fraud cases.

***Money Laundering*:** The stolen funds are transferred through a network of "mule accounts", often opened using fake or stolen identities. These accounts are used to Layer transactions, withdraw cash and transfer funds internationally. Law enforcement agencies have identified organised cyber crime networks using hundreds of mule accounts, thereby significantly complicating traceability and fund recovery efforts.

Real Case Examples from India

Case 1: Rs. 58 Crore Cyber Fraud Syndicate (Uttar Pradesh)

A cyber crime network defrauded victims of over Rs. 58 crore using phishing calls and fake banking alerts, using fake SIM identities, mule accounts and layered inter-state transactions. The case highlights the organised and networked nature of modern cyber crime beyond individual fraudsters.

Case 2: Investment Scam via Fake Trading Apps (Pan-India)

Victims were lured through social media advertisements and WhatsApp groups promising high stock returns. Fraudsters created realistic trading dashboards, showed fake profits and encouraged repeated investments, leading to significant financial losses and a major share of cyber crime-related damage.

Case 3: UPI Collect request Fraud

A victim approved a fake "refund" request and lost money, highlighting low awareness of push vs pull transactions in UPI. The National Cyber Crime Reporting Portal (NCRP) under the Ministry of Home Affairs (MHA) data shows over 36 lakh annual complaints, mostly linked to UPI, investment and OTP frauds - where high-frequency frauds are retail-based, while high-value frauds are investment or corporate -driven.

Emerging Trends in Modus Operandi

AI and Deepfake-based fraud: Cyber criminals are increasingly using AI tools to:

- Clone voices
- Create deepfake videos
- Impersonate executives

Cross-Border Operations: Many fraud networks operate from outside India, making jurisdictional enforcement difficult.

Automation and Scalability: Use of bots and automated calling systems allows fraudsters to target thousands of victims simultaneously.

The evolving nature of cyberfraud in India highlights the need for a comprehensive strategy combining technology, policy and user awareness. Early prevention - especially at the stages of social engineering and credential compromise - can significantly reduce losses. As threats evolve, adaptive and intelligence-driven security frameworks are essential to safeguard digital banking.

Role of Banks in Cyber Security

Banks are the primary defence in safeguarding the digital financial ecosystem, with roles extending to risk management, fraud prevention and customer protection amid rising digital transactions. They must adopt a multi-layered cyber security approach combining technology, regulation and user awareness, supported by the Reserve Bank of India guidelines, to remain resilient against evolving cyber threats.

Preventive Measures by Banks

Banks have implemented a range of preventive and proactive measures to mitigate cyber threats, focusing on both technological safeguards and behavioural risk management.

Multi-factor Authentication (MFA): MFA enhances banking security by requiring multiple identity checks (passwords, OTPs, biometrics or device authentication), reducing the risk of unauthorised access even if one credential is compromised. However, its effectiveness depends on user behaviour, as social engineering can still bypass it if users share OTPs.

Transaction Monitoring Systems: To identify odd trends, banks use sophisticated transaction monitoring systems that continually monitor customer behaviour. These systems examine variables including device usage location, frequency and transaction size. Early fraud detection is made possible by flagging suspicious transactions for additional verification.

Real-time fraud detection: Banks have implemented machine learning-powered real-time fraud detection systems in response to the growing speed of digital transactions, particularly through immediate payment

systems. These systems can minimise financial losses by promptly identifying irregularities and sending out notifications, blocking transactions or temporarily freezing accounts.

Tokenisation of card data: Tokenisation replaces sensitive card information with unique tokens during transactions, ensuring that actual card details are not exposed or stored. This significantly reduces the risk of data breaches and card-related fraud, particularly in online and contactless transactions.

Customer awareness campaigns: Banks actively carry out awareness efforts via SMS warnings, emails, ads and in-app notifications since they understand that a significant percentage of cyber fraud is caused by human mistakes. These campaigns educate customers about common fraud tactics, such as phishing and OTP scams and emphasize safe digital practices.

RBI Guidelines and Regulatory Framework

The Reserve Bank of India has established a comprehensive regulatory framework to strengthen cyber security in the banking sector, focusing on both prevention and customer protection.

Zero liability for customers in unauthorised transactions: RBI guidelines ensure that customers are not held liable for unauthorised transactions if they report the incident promptly and have not contributed to fraud through negligence. This provision enhances customer confidence and encourages timely reporting of cyber incidents.

Mandatory reporting timelines: Banks are required to report cyber fraud incidents within specified timelines to regulatory authorities. This facilitates faster investigation, enables coordinated responses and helps in building a centralized database of fraud patterns for better risk assessment.

Fraud monitoring systems: RBI mandates banks to establish robust fraud monitoring and risk management systems, including dedicated cyber security units and incident response teams. These systems are expected to incorporate advanced analytics, periodic audits and continuous surveillance to detect and mitigate threats effectively.

Banks play a critical and diverse role in combating cyber frauds in India. A well-rounded strategy that incorporates cutting-edge technology, legal compliance and consumer involvement is essential to their efficacy. Strengthening these systems will be crucial to ensure a safe, secure and trustworthy banking environment.

Preventive Measures for Individuals

In the context of rising cyber fraud, individual users play a crucial role in the first line of defence against cyber threats. In India, human mistakes, ignorance or behavioural manipulation account for a large percentage of cyber fraud instances rather than system malfunctions. Adopting secure digital practices is crucial as digital financial grow quickly, especially through platforms like the UPI. Preventive measures at the individual level can significantly reduce the likelihood of fraud and limit financial losses.

Some of the best practices for individuals are mentioned below:

- Never share OTP/ PIN
- Avoid unknown links/apps
- Verify UPI requests carefully
- Use official banking apps only
- Enable transaction alerts.

The effectiveness of cyber security ultimately

depends on the human element, often the weakest link. Despite advanced safeguards by banks and the Reserve Bank of India, many frauds exploit user behaviour through manipulation. Vigilant, informed users and continuous technological upgrades are essential to reduce cyber risks and ensure safe digital banking.

Role of Artificial Intelligence (AI) in Cyber Security

AI is transforming cyber security in banking by shifting from reactive to proactive risk management. With the rapid growth of digital transactions in India (especially UPI), AI enables real-fraud detection, faster response and improved accuracy by analysing large volumes of transaction and behavioural data.

Key application of AI

- *Fraud detection:* AI systems analyse transaction behavior instantly and flag suspicious payments.
- *Anomaly detection:* AI identifies unusual login patterns, device changes or abnormal spending behavior.
- *Predictive analytics:* Historical faud data is used to predict likely future attacks and vulnerable users.
- *NLP (Phishing detection):* AI scans emails, SMS and websites to identify phishing content.

Example: RBI-supported Digital Payments Intelligence Platform (DPIP) aims to improve real-time fraud coordination.

Broader Impact

Benefits: Faster detection, reduced losses, lower false alerts, scalability for millions of transactions.

Challenges: Deepfake misuse, privacy concerns, model bias, implementation cost and need for skilled workforce.

AI is, therefore, both a defensive necessity and an emerging strategic tool in modern banking cyber security. In India, the Reserve Bank of India is actively promoting AI-driven fraud monitoring systems such as the Digital Payments Intelligence Platform (DPIP) to improve real-time fraud detection and inter-bank coordination.

Strategies to minimise Cyber Frauds

In a rapidly digitizing economy like India, reducing cyber crime requires a coordinated and multi-layered approach involving banks, tech firms and the Government. With threats becoming dynamic and complex, the focus must shift to preventive, intelligence-driven and collaborative strategies supported by strong institutions, technology and regulations.

Policy–level Measures

At the macro level, Government and regulatory authorities play a critical role in shaping the cyber security landscape through legislation, enforcement and institutional coordination.

Strengthening Cyber laws: Robust and updated legal frameworks are essential to address emerging cyber threats such as AI-driven frauds, deep fakes and cross-border cyber crime, with stricter penalties and faster prosecution. Continuous updates by the Reserve Bank of India and other agencies are necessary to keep pace with evolving risks.

Faster grievance redressal mechanism: Timely response is crucial to recover funds in cyber fraud cases. Strengthening systems like the National Cyber Crime Reporting Portal (NCRP) and improving coordination among banks, regulators and law enforcement can ensure faster reporting, tracking and action.

Cross-border cooperation: As many cyber frauds originate from global networks, international collaboration, data-sharing and joint investigations

are essential to track and dismantle cyber crime syndicates and strengthen responses to transnational threats.

Bank-level Measures

Banks serve as the operational core of cyber security implementation and must adopt advanced tools and frameworks to detect and prevent frauds in real-time.

AI-based fraud monitoring: Banks are increasingly deploying AI and machine learning tools to monitor transactions continuously and detect suspicious patterns. These systems analyses large datasets in real-time, enabling early identification of fraudulent activities and immediate intervention. AI-driven monitoring enhances both speed and accuracy, reducing financial losses and improving customer protection.

Behavioral biometrics: Behavioral biometrics involves analyzing unique user behavior patterns such as typing speed, touch pressure, navigation habits and device usage. Unlike traditional authentication methods, this approach provides continuous verification throughout a session, making it highly effective in detecting account takeovers and unauthorized access.

Blockchain-based security: Blockchain technology offers a decentralized and tamper-resistant framework for secure transactions and data management. By ensuring transparency and immutability, blockchain can reduce fraud risks in areas such as payment processing, identity verification and record-keeping. Its application in banking can enhance trust and reduce the likelihood of data manipulation or unauthorised alterations.

Technology-level measures

Technological advancements are the backbone of modern cyber security systems, enabling secure communication, authentication and data protection.

End-to-end encryption: End-to-end encryption ensures that data transmitted between users and banks remains secure and cannot be intercepted or accessed by unauthorised parties. This is particularly critical for online banking, mobile applications and payment systems, where sensitive information such as account details and transaction data is exchanged.

Zero-trust architecture: Zero-trust security models operate on the principle of "never trust, always verify", requiring continuous authentication and authorisation for every access request. This approach minimises the risk of internal and external breaches by ensuring that no user or system is automatically trusted, regardless of their location or credentials.

Secure APIs: APIs are integral to modern banking, enabling integration with fintech platforms and third-party services. Securing APIs is essential to prevent unauthorised access and data breaches. This involves implementing strong authentication protocols, encryption and regular security testing to ensure safe data exchange.

Minimising cyber fraud requires a holistic strategy combining strong governance, advanced technology and proactive institutional measures. As threats grow, integrating AI, blockchain and secure systems – backed by robust policies - will be key to building a resilient financial ecosystem.

Key Findings

The study finds that cyber fraud in India has grown sharply alongside digital banking expansion, particularly through UPI, mobile banking and online payment channels. A large proportion of fraud cases are low-value retail incidents involving phishing, OTP theft, QR code scams and impersonation tactics, indicating that fraud is increasingly behaviour-driven rather than purely system-driven. While the number of

fraud cases has risen substantially, aggregate losses show signs of stabilization in some periods due to improved intervention systems and faster blocking mechanisms.

The study further find that high-value frauds are concentrated in investment scams and institutional lending irregularities, even though such cases are fewer in number. Banks are increasingly using artificial intelligence for real-time fraud monitoring, anomaly detection and transaction screening. However, low customer awareness, weak digital literacy and delayed reporting remain persistent structural vulnerabilities. Effective cyber security, therefore, requires coordinated action by regulators, banks, technology providers and customers. Behavioural biases such as trust, urgency, fear and greed significantly increase customer vulnerability to digital fraud. However, low customer awareness remains a major systemic weakness, increasing vulnerability to fraud.

Conclusion

Cyber security is now a critical pillar of financial stability in India's rapidly digitising banking system. While innovations like UPI improve inclusion and efficiency, they also increase vulnerabilities, with a shift towards high-volume retail frauds and high-value institutional frauds.

Addressing this requires an integrated approach – strong regulation, AI-driven technologies, robust banking controls and customer awareness. As threats evolve, a coordinated, proactive and intelligence-driven framework is essential to build resilience, sustain trust and support India's digital financial growth. The study examines cyber security in India's banking and digital payments ecosystem, focusing on retail fraud and institutional responses. The study has few limitations, including:

- Reliance on secondary data (with possible underreporting);
- Restricted access to bank-level data due to privacy.

Despite this, it offers a reliable and policy-relevant overview of cyber security challenges and strategic responses in India.

References

Aldasoro, I., Frost, J., Gambacorta, L. and Whyte, D. (2022), "Cyber risk, market failures, and financial stability", *Journal of Financial Stability*, Vol. 59, 000970, https://doi.org/10.1016/j.jfs.2021.100970.

Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T. and Savage, S. (2019), "Measuring the changing cost of cyber crime", *The Economics of Information Security and Privacy,* pp. 265–300.

Arner, D. W., Barberis, J. and Buckley, R. P. (2020), "FinTech, RegTech, and the reconceptualization of financial regulation", *Northwestern Journal of International Law & Business,* Vol. 37(3), pp. 371–413.

Bose, I. and Leung, A. C. (2023), "Cyber security in financial services: A review of risks and mitigation strategies", *Journal of Financial Crime,* Vol. 30(2), pp. 456–472, https://doi.org/10.1108/JFC-10-2022-0215.

Deloitte (2026), Behavioural Fraud Risk in Digital Banking.

Junger, M., Montoya, L. and Overink, F. (2017), "Priming and warnings are not effective to prevent social engineering attacks", *Computers in Human Behavior*, Vol. 66, pp. 75–87.

Kshetri, N. (2023), "Cyber crime and cyber security in India: Causes, consequences, and policy implications", *Telecommunications Policy*, Vol. 47(1), 102440, https://doi.org/10.1016/j.telpol.2022.102440.

Ministry of Home Affairs (2025), National Cyber Crime

Reporting Portal (NCRP) statistics.

National Crime Records Bureau (NCRB) (2024), Crime in India Report 2023.

NPCI (2025), UPI product Statistics, https://www.npci.org.in/what-we-do/upi/product-statistics.

PwC (2025), Global Economic Crime and Fraud Survey.

Reserve Bank of India (RBI) (2024), Report on Trend and Progress of Banking in India 2023-24, https://www.rbi.org.in/Scripts/AnnualPublications.aspx

Reserve Bank of India (2025), Annual report 2024-25.

Romanosky, S. (2016), "Examining the costs and causes of cyber incidents", *Journal of Cyber security*, Vol. 2(2), pp. 121–135.

The Wire Staff (2024, November 27), *India lost Rs 11,333 crore to cyber fraud in 2024: Report*. The Wire.