AN ANALYSIS OF THE CORRELATION BETWEEN DEVELOPMENT OF E-BANKING SYSTEMS AND GROWTH IN CYBER CRIME

Ayushi Belwal, Uttaranchal University

Dr. Anil Kumar, Uttaranchal University

Introduction

Indian banks face around 2,000 cyber attacks every hour. This makes banking security a major concern as we move deeper into the digital age. Digital banking has changed the way we handle our money and made banking more accessible than ever.

The shift to digital has created weak spots in our banking system. Looking at banking security across India shows a clear link between more people using e-banking and more cyber threats. India's challenges with building strong cyber security differ from countries like the UK and Singapore. The huge user base and mix of different demographics make security more complex.

Let's take a closer look at how e-banking systems have grown in India and track the rise in cybercrime. We'll assess how well current laws protect us and break down some key cases that show how cyber attacks on our banks are getting more sophisticated.

Abstract: Understanding the Link Between E-Banking and Cybercrime

E-banking growth and cybercrime create major challenges for financial institutions worldwide. E-banking offers convenience and flexibility through technology and has grown rapidly since the 1980s [1]. This digital shift has created weak spots that criminals exploit.

Banking sector cybercrime includes illegal activities carried out through global electronic networks [2]. These threats range from basic phishing scams to complex hacking attempts that steal data, interrupt services, or break into systems [3]. Banks face constant threats as attackers keep improving their methods to exploit system weaknesses [4].

Numbers tell a clear story about this growing threat. Cyberattacks in banking jumped 500%

between 2014-2019, with average losses of INR 1518.85 million per attack [3]. Banks make up 24.90% of all cybercrime targets, while social media accounts for 23.60% and webmail 19.60% [5]. India saw 3,855 financial cybercrimes and 534 phishing cases in 2020 alone [2].

These attacks mean more than just money lost. Security breaches hurt both banks and their customers through:

- Money losses for everyone involved
- Damage to reputation and customer trust
- Legal problems and regulatory fines
- Service disruptions
- Stolen customer data

"Computer impostors and criminals are few steps forward" despite security teams working hard to build safe platforms [2]. This ongoing battle keeps cybersecurity experts on their toes.

Developing economies like India face unique challenges with e-banking and cybercrime. Digital banking helps more people access financial services but creates new security risks. India deals with extra problems that developed countries don't face, such as poor facilities, limited networks, and unreliable power supply [1].

Criminals keep changing their tactics as technology advances. Mobile devices have led to more malware attacks [2]. Security experts warn of worse threats ahead, including DDoS attacks that could shut down multiple services at once [2].

Banking cybercrime poses unique challenges to police and security teams. Virtual crimes leave little evidence and cross borders easily. Criminals can attack from anywhere, making it hard to catch them [1].

Indian banks must balance security with accessibility. Their customers range from tech-savvy city dwellers to rural first-time users. Security needs to work and be easy to use. The real challenge lies in building complete security systems that handle technical, procedural, and human factors all at once.

Learning about how e-banking growth connects to rising cybercrime helps develop better protection for banks and customers while supporting digital progress.

Timeline of E-Banking Growth and Cybercrime Incidents in India

The rise of e-banking in India reflects a technological development that changed how financial services work. This transformation brought unprecedented convenience but also created new security challenges.

1996–2005: Early Internet Banking and Original Threats

ICICI Bank started India's e-banking experience in 1996. The bank offered simple features like account information access and basic correspondence [6]. Public adoption of internet banking picked up steam in 1999 as internet costs dropped and awareness grew [6]. Banks expanded their online services from information displays to transaction capabilities that included online bill payments and fund transfers [7].

The early 2000s saw banks putting money into technology infrastructure. Punjab National Bank led these investments according to the 2005 DQ-IDC Mega Spenders survey. The bank implemented digital certificates, SSL-enabled web servers, and mandatory password rotation policies [8]. These early security measures could not stop emerging threats. Over 1,000 phishing cases surfaced between December 2004 and March 2005 alone [8].

2006–2015: Rise of Mobile Banking and Phishing Attacks

Both e-banking adoption and cybersecurity incidents grew rapidly this decade. The Reserve Bank of India warned the public about phishing emails that claimed to offer "new online security protection" in early 2006 [9]. Online banking fraud losses jumped 55% in the first half of that year compared to the previous year [8].

Cybercriminals made their phishing attacks more sophisticated. They used social engineering and technical tricks to steal personal identity data and financial credentials from customers [10]. The '2005 India Web@work' survey showed that 32% of India's employees gave away confidential data including credit card numbers and corporate network passwords through phishing attacks [8].

Banking cybercrimes expanded beyond phishing by 2015. Criminals added malware, card skimming, and web application attacks to their arsenal. Verizon's data breach report in 2017 revealed these three attack types made up 88% of all security incidents in banking organizations [11]. CERT-In data showed phishing incidents in 2006 jumped 180% from 2005, and this trend continued [8].

2016–2024: UPI, FinTech, and Surge in Digital Frauds

UPI's launch in 2016 changed India's digital payment landscape and created massive growth in transaction volumes. UPI transactions grew by 137% between 2020 and 2022, reaching 200 trillion rupees [12]. The COVID-19 pandemic sped up banking digitalization and changed both back-end and front-end systems [13].

This rapid growth attracted cybercriminals. Union Bank of India lost INR 14,429.06 million in a devastating phishing email attack in July 2016 [13]. Digital payment fraud hit a record 14.57 billion rupees by 2024, which was five times higher than before [12].

Recent statistics tell a concerning story:

- UPI fraud incidents grew 85% in FY2023-24 compared to FY2022-23 [14]
- People reported 13.42 lakh UPI fraud cases worth Rs 1,087 crore in FY 2023-24 [14]
- Indian banks face 2,525 cyberattacks over six months—much higher than the global average of 1,674 attacks per organization, according to the Digital Threat Report 2024 [15]

Regulatory bodies responded with new rules. These included device binding requirements, two-factor authentication, daily transaction limits, and AI-based fraud monitoring solutions [16]. The government also created the National Cybercrime Reporting Portal and helpline number "1930" for reporting financial fraud [16].

Statistical Correlation Between E-Banking Usage and Cybercrime Cases

The link between e-banking adoption and cybercrime shows a worrying trend in Indian financial systems. Digital transactions have increased rapidly, and cyber attacks have become

more frequent and sophisticated. This has created new security challenges for the banking sector.

NCRB Data on Banking Fraud (2010–2023)

NCRB data reveals how cybercrime has evolved in India's banking sector. Cybercrime cases under the Information Technology Act jumped from 1,791 to 4,356 cases between 2010-2013 [5]. Cases reported to CERT-In grew from 22,060 in 2010 to 96,383 in 2013 [1]. The numbers kept climbing, with total fraud cases going up by 15% in 2018-19 [17].

These numbers are alarming not just because of their frequency but also their financial effect. Bank fraud values shot up from ₹1,999 crores in 2009-10 to ₹71,543 crores in 2018-19—a 35-fold increase [17]. A May 2023 survey found that 41% of people said their financial fraud cases hadn't been resolved, which shows how banks don't deal very well with these incidents [18].

RBI Reports on Digital Transaction Volume vs. Fraud Incidence

RBI data shows that more digital payments lead to more fraud incidents. Yes, it is true that digital technologies have cut transaction costs, but they've also created new weak spots [19]. This pattern became clearer during COVID-19, when people and businesses switched to contactless payments because of social distancing [19].

Latest RBI reports show bank frauds increased sharply in the first half of 2023-24, reaching 18,461 cases compared to 14,480 cases last year [4]. The financial damage jumped eightfold to ₹21,367 crore during this time [4]. These numbers prove that as digital transactions increase, cybercriminals get smarter too.

RBI's Financial Stability Report states that "with the rise in digital transactions, the volume of cyber frauds using novel modus operandi has increased in recent times" [4]. Therefore, regulators now focus on making the financial system safer and more resilient, especially when it comes to preventing fraud [4].

Comparative Analysis with UK and Singapore

Singapore and the UK have better systems to curb banking-related cybercrime than India's developing framework. Singapore ranks fourth highest worldwide in cybercrime victimization

rate—80% of its internet users have faced cybercrime [20]. The country has matched its laws with Budapest Convention requirements, letting it catch criminals wherever they are [20].

The UK uses a detailed approach through its National Cyber Security Strategy that focuses on detection, prevention, and response. Both countries have stronger cybersecurity systems than India, especially in catching criminals across borders.

India faces unique problems like not having up-to-the-minute fraud detection systems and limited power to prosecute international cybercrime. These weaknesses lead to fewer convictions in cybercrime cases and make India more vulnerable to threats like ransomware and complex phishing schemes.

Legal Frameworks Governing Cybersecurity in Indian Banking Sector

India has developed multiple frameworks to fight the growing cybercrime wave that protect banks and their customers. These legal structures are the foundations of cybersecurity in banking across the country.

Section 43 and 66 of IT Act, 2000

The Information Technology Act of 2000 (amended in 2008) is the life-blood of India's cybersecurity legal structure. Section 43 puts civil liability through financial penalties on unauthorized computer access and data theft. The section covers specific acts like:

- Unauthorized access to computer systems or networks
- Downloading or copying data without permission
- Introducing computer viruses or contaminants
- Disrupting computer systems or networks
- Denying authorized access to systems

People affected by these violations can claim compensation under Section 43. This helped in cases like the Reliance Jio data breach where the company used Section 43(2) after customer information showed up on an unauthorized website.

Section 66 makes these same acts criminal offenses when done "dishonestly or fraudulently." Violators face up to three years in jail or fines up to ₹5,00,000, or both. Section 66C punishes fraudulent use of electronic signatures or passwords, while Section 66D targets cheating through fake identities using computer resources.

RBI Cyber Security Framework (2016)

The Reserve Bank of India created its complete Cyber Security Framework in 2016 after several cybersecurity incidents. Banks must now:

- Create a board-approved cyber security policy separate from IT policies
- Set up Security Operations Centers (SOC) for constant monitoring
- Develop Cyber Crisis Management Plans (CCMP) for detection, response, recovery, and containment
- Put in place network and database security controls
- Protect customer information whatever the storage location

Banks must report all cybersecurity incidents to RBI, even failed attempts. Regular vulnerability testing is required. RBI emphasizes that "the nature of cyber-attacks are such that they can occur at any time and in a manner that may not have been anticipated."

RBI made these rules stronger in November 2023 through a master direction on "Information Technology Governance, Risk, Controls and Assurance Practices" starting April 1, 2024. Regulated entities now need three committees—IT strategy committee, IT steering committee, and information security committee—plus a chief information security officer.

CERT-In Guidelines and Compliance Requirements

The Indian Computer Emergency Response Team (CERT-In) was created under Section 70B of the IT Act as the national agency handling cybersecurity incidents. CERT-In's job includes:

- Collecting and analyzing cyber incident information

- Warning about possible threats
- Managing emergency responses
- Sharing guidelines and best practices

Banks must quickly tell CERT-In about cybersecurity incidents along with RBI, board members, management, and affected customers. CERT-In has special guidelines for government entities that set up "a prioritized baseline for cyber security measures and controls."

These three frameworks—IT Act provisions, RBI's Cyber Security Framework, and CERT-In requirements—work together to protect India's banking sector. Yet India still doesn't deal very well with enforcement, especially with cross-border cybercrimes and live fraud detection.

Singapore and the UK have better systems. Singapore lines up with the Budapest Convention giving it broad territorial reach. The UK's National Cyber Security Strategy focuses on detection, prevention, and response. These examples show what's possible as India keeps improving its legal framework to protect its fast-growing digital banking world.

Case Laws and Judicial Trends in Indian Cyber Banking Frauds

Recent court decisions have set crucial precedents for bank liability in cyber fraud cases in India. The courts now hold financial institutions more accountable to protect customer funds from unauthorized electronic transactions.

Punjab National Bank v. Ritu Mandal (2021)

The National Consumer Disputes Redressal Commission (NCDRC) made a groundbreaking ruling in January 2021. Banks must take responsibility for fraudulent withdrawals from customer accounts when these transactions happen without customer negligence [21]. The Commission directly cited the RBI circular dated July 6, 2017, which gives customers "zero liability" when banking systems show deficiencies [21]. This judgment created a powerful precedent that places technological responsibilities on banks instead of their customers.

ICICI Bank v. Shanti Devi (2019)

This case focused on how recovery agents hired by banks behaved. The respondent claimed her son took his own life after ICICI Bank's recovery agents barged into his bedroom. They harassed him about late payments and took away his motorcycle while his friends watched. This public humiliation ended up leading to his death [22].

The Supreme Court refused to remove the High Court's critical observations about the bank's collection methods. The Court stated that "the modus-operandi used by banks like ICICI for realization of their loan amount... is extra legal and by no stretch of imagination they can be permitted to hire musclemen and goons for recovery of their dues" [23]. The Court then stressed that financial institutions must follow legal procedures for loan recovery as outlined in the SARFAESI Act and RBI guidelines [23].

Analysis of Judicial Approach to Bank Liability

Indian courts have consistently reinforced several principles about bank liability in cybercrime cases:

Banks must use "the best of technology available today to detect and prevent unauthorized and fraudulent transactions" [2]. Courts have repeatedly emphasized that financial institutions, not customers, should handle technological responsibilities.

Justice Dharmesh Sharma's landmark ruling in the Delhi High Court in November 2024 made this clearer: "Security in digital banking is not solely about technology; it also involves the readiness of financial institutions to address risks and protect customers" [3]. This judgment shows that banks cannot shift their system failures onto customers without solid proof of negligence.

The Supreme Court made another key ruling in October 2024. They confirmed that "all transactions relating to the account of the respondent maintained with the petitioner-Bank were found to be unauthorized and fraudulent. The bank must take responsibility for such unauthorized and fraudulent transactions" [2].

These judgments show how Indian courts increasingly hold banks accountable in our digital financial world.

Materials and Methods: Data Sources and Analytical Approach

Our research combines multiple data sources and statistical tools to understand how e-banking adoption relates to cybercrime growth. Statistical correlations between digital banking growth and cybersecurity incidents emerge clearly from our analysis of data from trusted sources.

Data Collection from RBI, NCRB, and CERT-In

The research relies on data from several reliable sources. The Reserve Bank of India's annual reports provide detailed statistics about cybercrime incidents in the banking sector [24]. The National Crime Records Bureau (NCRB) records show cybercrime cases jumped by 63.5% in 2019 alone [25].

We gathered technical incident data from the Indian Computer Emergency Response Team (CERT-In). Their automated cyber threat exchange platform helps analyze threats proactively [26]. The Indian Cybercrime Coordination Center's (I4C) data proved valuable, especially their National Cyber Crime Reporting Portal. The portal's statistics reveal around 100,000 cyber complaints registered since January 2023 [15].

Methodology: Regression Analysis and Trend Mapping

We used multiple regression analysis in the Statistical Package for Social Science environment to study how financial losses connect with cybercrime activities [27]. This helps us calculate the relationship between independent variables (online banking fraud and mobile banking fraud) and the dependent variable (financial losses) [28].

Our analytical framework has:

1. Descriptive statistical analysis that shows percentage growth rates in cybercrimes
2. Comparative analysis between public and private sector banks' vulnerability patterns
3. Trend mapping to spot emerging threat vectors

Our regression model showed a coefficient of B=0.445 (p=0.000), revealing how cybercrime techniques affect online banking usage [28]. We created scatterplots through linear regression to

visualize correlations. The dependent variable (Y) shows measurable impacts while independent variables (X) represent specific cybercrime factors [29].

The analysis managed to keep track of both direct financial impacts and secondary effects like reputation damage and operational disruptions that affect banking sector's cybersecurity.

Limitations in Current Cybersecurity and Legal Enforcement

India's cybersecurity enforcement has serious problems despite having many regulations. Even the best legal provisions don't protect institutions and customers from new threats.

Lack of Live Fraud Detection Infrastructure

Indian banks' fraud detection systems mostly use batch processing. This outdated method spots fraud hours or even days after it happens. By that time, criminals usually escape with large amounts of money [11]. Banks don't deal very well with live analytics because they face resource limits and technical problems with their core banking systems. Small financial institutions find it especially hard to pay for modern cybersecurity solutions [30]. So many banks don't have the tools to spot threats instantly, which gives cybercriminals their chance to strike.

Jurisdictional Challenges in Cross-Border Cybercrime

Indian authorities face huge problems fighting cross-border cybercrime. Of course, cyberspace has no borders, which creates jurisdictional headaches when chasing criminals operating from other countries [6]. We don't have proper legal systems to collect and share digital evidence across borders [31]. Working with other countries is vital, but different legal systems, privacy laws, and political issues make it hard for police agencies to share information [6]. On top of that, legal help requests between countries take too long and don't work well [31].

Low Conviction Rates in Cybercrime Cases

The most worrying fact is that India's cybercrime conviction rates are extremely low. Official data shows:

- Between 2020-2022, only 2,706 people (1.6%) were convicted out of 1.67 lakh registered cybercrime cases [32]

- The conviction rate dropped to just 0.93% of registered cases in 2021 [32]
- Only 1.7% of cybercrime cases led to convictions in 2022 [32]

Several factors cause these low conviction rates. We found that investigation teams lack the technical skills to collect, track, and analyze digital evidence properly [33]. Digital evidence can disappear or get hidden before trials start [33]. More than that, courts don't understand digital evidence well enough [34]. Cases often get stuck forever because there's no standard way to collect and analyze digital evidence [34].

Conclusion

Data shows a clear link between the rise in e-banking and cybercrime across India's financial sector. Indian banks face about 2,000 cyber attacks every hour. The conviction rate in cybercrime cases stays below 2%. These numbers reveal major gaps between technology advances and security measures.

Landmark court decisions like Punjab National Bank v. Ritu Mandal (2021) and ICICI Bank v. Shanti Devi (2019) have set vital precedents that make banks more responsible for protecting their customers. RBI's Cyber Security Framework provides detailed guidelines, but smaller banks with limited resources don't deal very well with implementation.

India's cybersecurity framework needs to be much stronger than its current state, especially when compared to Singapore and the UK. Singapore works with the Budapest Convention while the UK's National Cyber Security Strategy offers great lessons to improve India's system.

The banking sector and policymakers must focus urgently on three key areas:

- Building reliable real-time fraud detection systems
- Better capabilities to investigate cross-border cybercrime
- Law enforcement agencies' technical expertise

A coordinated approach between banks, regulators, and law enforcement can help tackle these challenges effectively. Banks should invest more in cybersecurity while keeping their services

user-friendly for India's diverse population. The legal system also needs regular updates to handle new cyber threats.

Secure e-banking's future in India depends on striking the right balance between digital breakthroughs and reliable security measures. India can build a stronger digital banking system through better technology, stronger law enforcement, and international teamwork. This will protect both banks and customers from evolving cyber threats.

References

[1] - https://cis-india.org/internet-governance/files/india-uk-legal-regulatory-approaches.pdf
[2] - https://m.economictimes.com/wealth/save/cyber-fraud-supreme-court-orders-sbi-to-refund-rs-94000-lost-in-an-online-scam-to-its-customer/articleshow/117022936.cms
[3] - https://www.acmlegal.org/blog/justice-in-the-digital-age-a-landmark-judgment-on-cyber-fraud-by-the-delhi-high-court/
[4] - https://www.cnbctv18.com/technology/rbi-report-stresses-need-for-public-awareness-about-cyber-frauds-19531944.htm
[5] - https://ncrb.gov.in/
[6] - https://theamikusqriae.com/jurisdictional-challenges-in-cyber-crimes-issues-with-cyber-crimes-that-transcend-national-borders/
[7] - https://www.icommercecentral.com/open-access/adoption-of-internet-banking-an-empirical-investigation-of-indian-banking-sector.php?aid=38659
[8] - https://www.icommercecentral.com/open-access/online-frauds-in-banks-with-phishing.php?aid=38493
[9] - https://www.rbi.org.in/commonman/english/scripts/PressReleases.aspx?Id=2438
[10] - https://corp.onlinesbi.sbi/corporate/sbi/corp_aboutphishing.html
[11] - https://sigmoidanalytics.medium.com/ai-enabled-real-time-analytics-improves-fraud-detection-for-banks-962da5479094
[12] - https://www.businesstoday.in/technology/news/story/digital-payment-frauds-surge-in-india-as-upi-transactions-skyrocket-rbi-report-431695-2024-06-01
[13]https://www.researchgate.net/publication/385879394_ANALYZING_CYBERCRIMES_AND_CYBER_SECURITY_LANDSCAPE_IN_THE_BANKING_SECTOR_OF_INDIA
[14] - https://www.medianama.com/2024/11/223-upi-fraud-up-85-per-cent-fy2023-24-finance-ministry-data/
[15] - https://ijirt.org/publishedpaper/IJIRT171471_PAPER.pdf
[16] - https://pib.gov.in/PressReleasePage.aspx?PRID=2110405
[17] - https://factly.in/amount-involved-in-bank-fraud-cases-increased-35-times-in-10-years/
[18] - https://www.statista.com/statistics/1394717/india-money-recovery-after-financial-fraud/
[19] - https://rbi.org.in/scripts/PublicationsView.aspx?Id=22459
[20]https://www.researchgate.net/publication/292471148_Cyber_crime_in_Singapore_An_analysis_of_regulation_based_on_lessig's_four_modalities_of_constraint

[21] - https://www.livelaw.in/top-stories/supreme-court-explainer-consumer-and-bank-liability-in-case-of-fraudulent-unauthorized-transactions-281236
[22] - https://unfoldlaw.in/icici-bank-vs-shanti-devi-sharma-others/
[23] - https://indiankanoon.org/doc/1515197/
[24] - https://www.jetir.org/papers/JETIR2405H37.pdf
[25] - https://www.jetir.org/papers/JETIR2012332.pdf
[26] - https://www.mha.gov.in/MHA1/Par2017/pdfs/par2023-pdfs/LS-08082023/278.pdf
[27] - https://www.emerald.com/insight/content/doi/10.1108/jfc-04-2023-0094/full/pdf?title=analysis-of-cyberfraud-in-the-south-african-banking-industry-a-multiple-regression-approach
[28]https://www.researchgate.net/publication/369090232_Cybercrime_Techniques_in_Online_Banking
[29] - https://www.ripublication.com/ijsa21/ijsav11n1_02.pdf
[30] - https://ijirl.com/wp-content/uploads/2024/12/E-BANKING-IN-INDIA-AN-ANALYSIS-OF-REGULATORY-FRAMEWORK-AND-COMPLIANCE-CHALLENGES.pdf
[31] - https://www.researchgate.net/publication/389416219_Cross-Border_E-Crimes_Jurisdiction_and_Due_Process_Challenges
[32] - https://www.tribuneindia.com/news/india/only-1-6-conviction-rate-in-2-yrs-amid-surge-in-cybercrime-cases-2/
[33] - https://ksandk.com/information-technology/low-cyber-crime-convictions-india/
[34] - https://www.livemint.com/Home-Page/6Tzx7n4mD1vpyQCOfATbxO/Why-most-cyber-crimes-in-India-dont-end-in-conviction.html