Page 2558 - 2562 **DOI:** *https://doij.org/10.10000/IJLMH.119358*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 2

2025

An Analytical Study of the Economical Setbacks Faced by the Indian Banking Sector due to the Surge of Cyber Crimes

ADITI SRIVASTAVA[1] AND RATNESH KUMAR SRIVASTAVA[2]

ABSTRACT

The introduction of technology and its astronomical use in the society proves to be both a boon and a bane. The 21st century is already known to be the age of advanced technology where the newly invented technologies aim at providing easier standards of living. This advancement of technology simultaneously leads to the growing concern of its misuse against an individual or the society at large. The ever-evolving nature of the Internet of Things (IoT) backed by evolving technologies creates a breeding ground for the cybercrime perpetrators. The rise in technology has left no sector untouched and one of these sectors comprise of the Banking Industry. The banking industry in India forms the backbone of the economy of the nation. The Indian Banking sector has undergone various transformations and one of the significant transformations is the digitization of this sector. With the increase of digitisation of the banks, this sector simultaneously witnessed the surge of cybercrimes making its headlines not only in India but worldwide. This article aims to focus upon the vulnerabilities of the banking sector against the rampant increase of cybercrimes which ultimately leads to the economic losses to a large extent. With India set to become a 5.7 trillion-dollar economy by 2028, according to Economic Times, increasing number of cybercriminal activities pose a potential threat to India's economy. This article aims to highlight the economic setbacks faced by the Indian Banks due to the increasing surge of cybercrimes and evaluate the legal framework along with the strategies to mitigate the risk of cybercrimes in the Indian Banking sector.

Keywords*: Cybercrime, Banking Sector, Indian Economy, Digitization.*

I. INTRODUCTION

The modus operandi of the Banking sector in India has undergone a major shift from the conventional walk-in service availment to digitalised financial transactions. Banking has come a long way from the time of ledger cards and other manual filing systems to the computer age. Computerisation in the Indian banking industry was introduced first in 1970s by Societe

[1] Author is a student at Law College Dehradun, faculty of Uttaranchal University, India.
[2] Author is an Assistant Professor at Law College Dehradun, faculty of Uttaranchal University, India.

 [ISSN 2581-5369]

Generale Bank (India) Ltd. Until the mid-1990, few banks that were computerised adopted the Local Area Network (LAN) within the bank branches. The sophisticated ones among the banks then implemented the Wide Area Network (WAN) by linking branches within cities while some implemented intercity connectivity using leased lines.[3] After the outbreak of Covid-19, there was a major shift towards the rapid digitalization of banking services and its availment by the masses situated even at the remote areas. With India being the second-largest internet population in the world[4], it becomes more vulnerable to the risks of cybercriminal activities. A cybercrime, simply means, a criminal activity carried out by an individual or group or an organisation using computer as both the means and the target. The omnipresence of internet at every Indian household have not only made lives of people easier but also aggravated the risk of cybercriminal attacks by the perpetrators of crime who have shifted from committing crimes using conventional methods to a much more convenient and sophisticated means, that is Internet.

The banking sector has already seen a rapid spike in the cybercrimes objected towards it after the rampant digitalisation focussing on conducting online transactions. According to data from the Reserve Bank of India, sent in response to the authors' Right to Information (RTI) application, ₹3,207 crore was lost because of 5,82,000 cases of cyber fraud between FY2020 and FY2024.[5] This data proves the fact that cybercrimes targeting the banking industry has caused substantial economic losses and would continue to do so unless a robust cybersecurity measure is adopted.

II. CYBERCRIMES IN THE CONTEXT OF THE INDIAN BANKING SECTOR

Cybercrimes are crimes which are committed using a computer. Cybercrimes pose a threat to Indian digital transformation initiatives. The increasing malicious use of the Internet to commit cybercrimes causes fear and may deter citizens and businesses from embracing digital technologies, stifling progress, and hindering the potential benefits of a digital economy. This poses a potential challenge as India aims to increase use of technology for governance, online services, and digital payments.

The ever-evolving technologies have led to the development of newer varieties of cybercrimes

[3] R.O. Salawu and M.K. Salawu, "*The Emergence of Internet Banking in Nigeria: An appraisal*", (2007) 6 Information Technology Journal (Issue 4), pp. 490-496.
[4] *Cyber crime in India*. Available at: https://www.statista.com/topics/5054/cyber-crime-in-india/ (Accessed: 13 April 2025).
[5] Md Zakaria Siddiqui & Sabir Ahamed, *Cyber Fraud in Banking Transactions Surges in FY24: Data*, THE HINDU, Nov. 5, 2024, https://www.thehindu.com/data/cyber-fraud-in-banking-transactions-surges-in-fy24-data/article68813626.ece (last visited Apr 13, 2025).

 [ISSN 2581-5369]

which makes it difficult for the cybersecurity agencies to function and trace the perpetrators. In today's fast-paced digitalised world, online financial transactions such as net-banking, bank specific mobile apps, and digital wallets gain prominence. Cybercriminals find new techniques and ways to exploit the vulnerabilities in the Banking Sector. According to research from the Reserve Bank of India (RBI), the country's digital payment ecosystem expanded by approximately 55% between 2021 and 2023. Some of the cybercrimes affecting the Indian Banking Sector are:

- Fraud- A fraud is caused by wrongfully causing loss to a person by using dishonest means. Cybercriminals defraud the banks and its customers by stealing debit/credit card details in the pretext of providing a service gaining unauthorised access and causing financial losses. The Data submitted by the finance ministry to parliament on Monday showed that people lost a combined 1.77 billion rupees ($20.3 million) to fraud in the fiscal year ended March 2024.[6]
- Identity theft- Every Indian Bank requires Aadhar Card and PAN Card during registration of its customers and hence, retrieves such data in their systems for record. Cybercriminals steal personal information to create fake personality and apply for loans, credit cards, etc., which when defaulted constitute the Non-Performing Assests of the Bank and cause financial loss to the banks.
- Denial of Service Attacks (DoS) and Distributed Denial of Service (DDoS) Attacks- Such attacks block the bank's servers with a flood of excessive traffic causing systems to disfunction temporarily. These types of attacks are quite common within payment gateways and used to disrupt online banking services.
- Phishing scams- The most dangerous frauds that causes in day-to-day banking activity is phishing, a criminal activity using social engineering techniques.[7] Phishing is a fraudulent attempt to retrieve sensitive bank information, such as OTPs, login credentials, and credit card details by impersonating a trusted entity through emails, SMS, fake websites, or pop-ups. If a user opens such fake websites, etc., it will lead to unauthorized transactions, identity theft and financial loss to a large extent.
- Ransomware attacks- Ransomware is a type of malware or a computer virus which

[6] www.ETTelecom.com, *Govt Says Cyber Fraud Cases Jumped over Four-Fold in FY24, Caused $20 Million Losses - ET Telecom*, ETTELECOM.COM, https://telecom.economictimes.indiatimes.com/news/internet/govt-says-cyber-fraud-cases-jumped-over-four-fold-in-fy24-caused-20-million-losses/118882311 (last visited Apr 13, 2025).

[7] ***Critical Analysis of Cyber and Banking Financial Frauds in Relation to Technology*, (2023) PL January 62 at page 65**

 [ISSN 2581-5369]

encrypts a bank's system or important data and makes it unavailable or inaccessible until a ransom is paid to the cybercriminals responsible for such attacks.

- Man-in-the-Middle (MITM) Attacks- In such attacks, the hackers trace the communications made between the bank and the custormers to steal sensitive information or manipulate transactions. These types of attacks occur mainly through unsecured public Wi-Fi networks.
- Cybercrime using Artificial Intelligence- Cybercriminals now, keeping at par with the technological advancements, use Artificial Intelligence and Deep Fake technology to commit cybercrimes by creating fake audio-video for deceiving the banking officals as well as its customers.

Such cybercrimes target the banking sector in order to drain them financially. The cybercriminal attacks are not only limited to causing of financial losses but adversely affect the bank-consumer relationship, disempowering the belief system of the public on online transactions and net banking services. Perceived risk is one of the main inhibitors for internet banking usage and can be described as a customer's opinion of uncertainty and probable negative consequences of making use of internet banking.[8] In addition to this, The National Crime Records Bureau (NCRB) data shows a 60% year-on-year rise in cyber crimes affecting financial platforms.

III. REASONS BEHIND THE INCREASE IN CYBERCRIMES TARGETING THE BANKING SECTOR

There are various reasons backing the increase in cyber crime rates targeting the Banking sector and causing it financial losses. Some of the reasons are highlighted below:

1. Rapid Digitalisation- The Digital India Initiative by the Government of India has contributed in the rapid digitalisation of all the sectors with the banking sector being one of them. There came an aggressive push towards cashless economy after the outbreak of COVID-19 where people were forced to remain at their homes with minimal contact with the surroundings and then, the internet banking became a need rather than a choice.
2. Technological Advancements- With the development in the technology and with an increase in the inflow of the novel technologies, the cybercrime perpetrators have managed to match with the technological advancements and to commit cybercrimes using technology as their instrument with the latest being the use of Deepfake

[8] J.RS. Fonseca, *E-banking culture : A comparison of EU 27 countries and Portuguese case in the EU 27 retail banking context*, 21 Journal of Retailing and Consumer Services, 708 (2014), 709, available at https://www.sciencedirect.com/science/article/abs/pii/S096969891400068X. last seen on 21/03/2025

 [ISSN 2581-5369]

technology and Artificial Intelligence.

Poor Cybersecurity measures- With the inoculation of internet at the remotest of the areas in India and India being the second largest Internet consumer, it still lacks the infrastructure and the trained taskforce needed to curb the menace of cybercriminal activities which gains momentum due to the use of weak cybersecurity measures and older technology to trace the cybercrime perpetrators.

*****

 [ISSN 2581-5369]