© December 2025 | DC2501| Volume 1 | Issue 2 | ISSN: ISSN: 3107-7536 (Online)
Vyavahāra: International Journal of Commerce, Ethics, Law & Management

Cyber Security Issues in online financial transaction in India: A study with reference to 2019-2024

Dr. V. Prabakaran[1], Mr. S Arun Sathappan[2]
Head of the Department[1], Student[2]
Department of Commerce (Honours) - International Accounting and Finance
Faculty of Science and Humanities
SRM Institute of Science and Technology, Chennai
prabakav1@srmist.edu.in, as1436@srmist.edu.in

Abstract

The Indian financial transaction system has undergone a substantial transformation due to the swift expansion of digitalization. India has been targeted by cyber threats for many years, particularly as a result of the rapid growth of digital payment systems over the last several years. Cyber security issues associated with online financial transactions in India will be the subject of this research study conducted between 2019 and 2024. This research study will utilize only secondary sources of information collected from reports issued by the Reserve Bank of India governmental publications, scholarly journals, academic research papers, and reputable Internet websites. All collected data has undergone systematic review and analysis in order to better understand how and where the growth of digital payment systems has occurred as well as what types of cyber security risks are associated with the expansion of modern systems. This paper explores numerous examples of potential threats to online transactions through computer systems and networks. The examples highlighted include identity theft via malware attacks, online banking fraud, card-related or UPI scams, phishing attacks, and the various methods of perpetrating all of the above. In addition to demonstrating how victims are affected by these cyber threats, this paper also evaluates how they result in financial loss or inadequate customer trust for those affected through the misuse of their data. The paper also reviews India's Cyber Security and Regulatory Frameworks in light of such challenges. In this regard, it proposes improved security for financial transactions through technology

Keywords: Cyber security, Block Chain, Digital Transaction, Online Financial Transaction\

1. Introduction

The world of finance is changing fast, and India is right at the heart of this digital revolution. Today, things like UPI, mobile wallets, and internet banking are part of our everyday lives. Thanks to government pushes like "Digital India," better internet, and everyone having a smartphone, these services have become incredibly easy to use from anywhere at any time. But this heavy reliance on digital tools has a downside: a growing worry about cybersecurity. Risks like phishing, malware, and fraud are real threats to our money and our private data.

1.2 Need for the Study

As digital payments explode in popularity, they also become bigger targets for hackers. We need this study to understand these new risks, find the weak spots in our current systems, and figure out how to keep transactions safe.

1.3 Influence (Impact)

Cyberattacks do more than just steal money; they ruin the reputation of banks and make people lose faith in digital payments. The rise in fraud shows we need better security and much more awareness for both regular people and big organizations.

1.4 Statement of the Problem

Even though digital transactions are booming in India, so are cybercrimes like data breaches and phishing. The problem is twofold: many users don't know how to stay safe, and our financial systems are still struggling to keep up with increasingly sophisticated attacks.

1.5 Theoretical Framework:

This study is built on a simple idea: the more we use digital payments, the more we are exposed to cyber risks. To protect this ecosystem, we need three main things: strong security frameworks, clear government rules, and users who know what to look out for.

1.6 Significance of the Study

This research is meant to be a guide for banks, policymakers, and everyday users. By identifying the biggest threats, we can work together to build a safer digital financial world in India.

1.7 Objectives:

- To analyze the growth of online financial transactions in India
- To identify the major cyber security threats affecting online financial transactions

1.8 Scope of the Study

We are focusing specifically on cybersecurity issues within India's digital payment landscape between 2019 and 2024, looking at how adoption trends and fraud cases have changed over those five years.

2. Scholarly Review

The rapid increase in online financial transactions has also created new threats to cyber security., **Alkhalil et.al (2021)** studied the number of phishing attacks and determined that they are among the most common types of cyber threats to online financial transactions. Cyber criminals who commit these types of crimes scam users into providing them with sensitive financial information (e.g., user IDs, passwords, and bank account numbers) by sending emails with bogus hyperlinks or leading users to malicious websites.According to Alkhalil's research, a lack of awareness of security protocols has rendered most digital payment systems vulnerable to cyber-attack.

In **Cook (2019)**, studied the evolution of digital payments in the country of India. He reported that the National Payments Corporation of India (NPCI) is implementing several initiatives to facilitate the evolution of digital payment systems, including the Unified Payments Interface (UPI), Real Time Gross Settlement (RTGS), Immediate Payment Service (IMPS), and RuPay card network. The growth of such technologies has given rise to an abundance of convenience and, simultaneously, has significantly increased the likelihood of cyber-crimes (phishing and transaction fraud) occurring.Cook contends that the government should establish regulatory guidelines and mandate that payment systems enhance their cybersecurity infrastructure.

According to recent research conducted by **the Reserve Bank of India (2022)**, there has been a rapid rise in the use of digital payment systems across India and it has been recognized that strong cybersecurity frameworks would be essential for protecting electronic payments. The report highlighted some of the major risks including transaction fraud, phishing and vulnerability of systems. It recommended implementing risk management systems, continuous monitoring and consumer awareness programs as a means to improve security. Research conducted **by Kumar (2020)** on the perceptions of e-banking users regarding security suggested that security related to data breaches and financial fraud is likely to be among the greatest influencers on the acceptance of digital banking services. This research also observed that the implementation of next-generation authentication systems (e.g., encryption and two-factor authentication) has a high probability of improving consumer confidence in the use of electronic financial services.

In summary, while digital payments have improved the access and efficiency of financial services, they have also presented a number of serious cybersecurity issues. Therefore, continued improvement to the security infrastructure, regulatory policies and consumer education is essential to provide a level of protection for electronic financial transactions.

3. Research Methodology

3.1 Research Design

To get a clear picture of what's happening, we used a descriptive research design. This approach is perfect for spotting trends and seeing how the rise in digital payments links up with the rise in cyber threats between 2019 and 2024.

3.2 Nature of Data

This study relies on secondary data information that has already been gathered and shared by experts and institutions. This is the best way to handle large scale national statistics.

3.3 Sources of Data

- **Government Reports:** Insights from the RBI and the Ministry of Electronics and Information Technology.
- **Financial Reports:** Statistics from the NPCI.

- **Academic and Industry Reports:** Scholarly journals and studies from the cybersecurity industry.

3.4 Period of Study

We looked at the years 2019 to 2024 a time of explosive growth for UPI and mobile banking, but also a time when cyber threats became much more common.

3.5 Tools Used for Data Analysis

To make the data easy to understand, we used visual tools like line graphs, bar charts, and trend analysis. These help us clearly show how digital growth and fraud are moving together.

Category	Component	Details
Research Framework	Research Design	A Nominal research design has been used to analyze cyber security issues in the Online digital financial transactions
Data Type	Nature of Data	The Secondary data has been collected from Different sources such as the RBI, Cybercrime reports and financial intuition reports
Data Sources	Sources of Data	The Data are collected from the Government and Other Corporate publication such as the RBI, Academic Journals, cyber security reports
Study Duration	Period of Study	The Period of study was between 2019-2024 analyzing the patterns and the data of the cyber security and its users along with the increasing fraud and phishing attack and many other cyber attacks that have been evolving
Analytical Methods	Tools Used	Graphical analysis including line graphs, bar charts, and trend analysis

Research Framework Table

The research Framework table consist of the Combination of the two Graph that shows the combination of the line and bra a clustered one showing all the data and helped in the observation of the patters and also helped in mapping the data in a timely interval

Table 1: Trends in Digital Transactions, Cyber Fraud Cases, Financial Loss, and UPI Transactions in India (2019–2024)

Year	Digital Transactions (Billion)	Cyber Fraud Cases	Financial Loss (₹ Crore)	UPI Transactions (Billions)
2019	34	44,546	120	5.3
2020	44	65,893	185	12.5
2021	56	85,430	320	38.7
2022	74	98,765	510	74
2023	94	1,25,672	780	117
2024	120	1,42,450	950	140

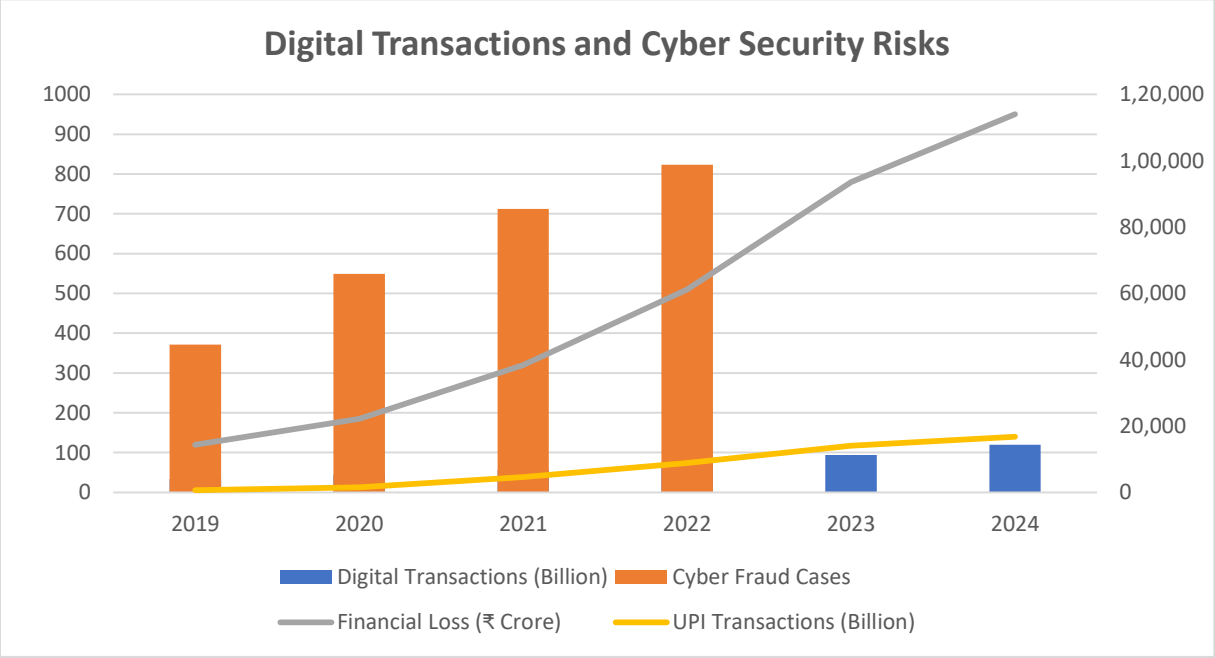

Figure 1: Growth of Digital Transactions and Cyber Security Risks in India (2019–2024)

Source: Secondary Data / RBI Reports / Cyber Crime Reports

The graph shows the trend of digital financial transactions and cyber security risks in India from 2019 to 2024. The number of digital transactions increased significantly during this period, indicating the rapid growth of digital payment systems. UPI transactions also experienced substantial growth, reflecting the increasing popularity of instant digital payment platforms. At the same time, cyber fraud cases have risen considerably, highlighting the growing risks associated with online financial activities. Financial losses due to cyber-crimes have also

increased over the years. The trend also suggest strong cyber crime laws and security are essential.

Table 2: Growth of Internet Users, Digital Wallet Users, and Cyber Security Threats in India (2019–2024)

Year	Wallet Users (Million)	Fraud Cases	Phishing Attacks	Internet Users (Million)
2019	250	18,500	52,000	504
2020	300	27,200	71,000	622
2021	350	34,000	95,000	692
2022	420	41,600	1,20,000	759
2023	480	56,800	1,48,000	820
2024	540	63,000	1,75,000	880

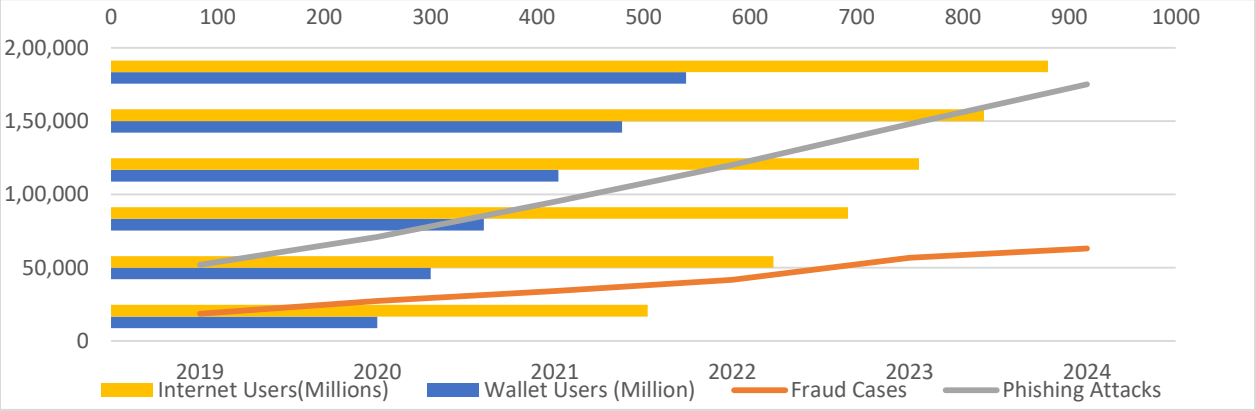

Figure 2: Growth of Internet Usage, Digital Wallet Adoption, and Cyber Security Threats in India (2019-2024)

Source: Secondary Data compiled from reports of the Reserve Bank of India (RBI)

The graph illustrates the growth of internet users and digital wallet adoption in India from 2019 to 2024. The number of internet users increased steadily during this period, contributing to the expansion of digital financial services. The number of digital wallet users also showed a consistent rise, indicating the growing acceptance of mobile-based payment systems

significantly. Phishing attacks has shown a sharp rise with online financial transactions. Laws and Regulation must be strict in order to reduce the cyber attacks and fraud in Online digital Transactions

5. Conclusion

5.1 Major Findings of the Study

Looking back at 2019–2024, the numbers tell a story of incredible progress and rising risk. Digital transactions jumped from 34 billion to 120 billion, and UPI transactions saw an even bigger leap from 5.3 billion to 140 billion. But the "dark side" of this growth is that fraud cases more than tripled, and financial losses soared from ₹120 crore to ₹950 crore. We found that phishing, identity theft, and malware are the biggest threats today. These findings echo what other experts have said: as we expand our digital world, the risks follow.

5.2 Suggestions and Recommendations

For Government and Regulatory Authorities:

The RBI and the government should keep sharpening their policies. This means setting higher security standards for banks, improving how we track cybercrime, and pushing for the latest security tech.

For Users and the General Public:

Safety starts with us. We must never share passwords or OTPs with anyone. Using secure networks, keeping apps updated, and double -checking payment links can save us from becoming another statistic.

5.3 Limitations of the Study

This study is based on existing data and focuses only on India from 2019 to 2024, so it might not cover every possible scenario or other regions.

5.4 Conclusion

Digital finance has made our lives easier, but it has also brought new dangers. If we want a digital economy that lasts, we have to invest in better regulations, smarter technology, and,

most importantly, making sure every user knows how to stay safe. This study also mainly emphasis the importance of the Regulation system and laws which has to be made in order to make the digital payment system sooth and make a easier payment without any frauds and crime and also cyber attacks

Reference:

- Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in ComputerScience,3,563060. https://doi.org/10.3389/fcomp.2021.563060
- Böhme, R., & Moore, T. (2019). The economics of cybersecurity: Principles and policy options. International Journal of Critical Infrastructure Protection, 25, 1–8. https://doi.org/10.1016/j.ijcip.2019.02.001
- Cook, W. (2019). The rise of digital payments in India and its implications for financial inclusion. Journal of Payments Strategy & Systems, 13 (3), 210–221.
- IBM Security. (2023). Cost of a data breach report 2023. IBM Corporation. https://www.ibm.com/security
- Kshetri, N. (2021). Cybercrime and cybersecurity in the global financial sector. Computer, 54 (8), 20–27. https://doi.org/10.1109/MC.2021.3093745
- Kumar, A. (2020). Security perception and adoption of internet banking in India. International Journal of Bank Marketing, 38 (4), 1001–1019. https://doi.org/10.1108/IJBM_09_2019_0332
- MeitY. (2022). Cyber security policy and initiatives in India . Ministry of Electronics and Information Technology, Government of India. https://www.meity.gov.in
- National Payments Corporation of India. (2023). UPI product statistics. NPCI. [suspicious link removed]
- Organization for Economic Cooperation and Development. (2020). Digital security risk management in finance. OECD Publishing. https://www.oecd.org
- Reserve Bank of India. (2022). Annual report 2021–22. Reserve Bank of India. https://www.rbi.org.in
- Statista. (2024). Digital payments in India – Statistics and facts . Statista Research Department. https://www.statista.com
- World Bank. (2021). Digital financial services. World Bank Group. https://www.worldbank.org