JOURNAL OF CYBER COVERNANCE AND INTELLECTUAL PROPERTY

Volume 1 Article 19

Cyber Fraud and Digital Payment Security Regulations

Deeya Thapa

University of North Bengal

Recommended Citation:

Thapa (2026) "Cyber Fraud and Digital Payment Security Regulations" Journal of Cyber Governance and Intellectual Property, Vol. 1, Article 19. (DOI)

ABSTRACT

With the rapid growth of technology, digital payment systems such as mobile banking, QR codes, and Unified Payments Interface (UPI) have become an essential part of everyday transactions including shopping and basic purchases. However, this increasing dependence on digital platforms has also led to a rise in cyber frauds, including online financial fraud, identity theft, spyware attacks, and other forms of cybercrime targeting users through applications, browsers, and websites. As a result, there is a need for secure digital payment systems to safeguard users from emerging cyber threats. This study examines the regulatory framework governing cyber fraud and digital payment security in India. It analyzes key legal provisions such as the Information Technology Act, 2000 and Digital payments security guidelines issued by the Reserve Bank of India. Although India has a strong legal framework to address cyber fraud, there are certain gaps in the provisions. This study focuses on identifying these gaps and evaluating the need for strengthening the regulatory framework to protect the users from any kind of cyber fraud and ensure greater security in digital transactions.

KEYWORDS

Cyber Fraud, Digital Payment Security, Information Technology Act, 2000, Reserve Bank of India, Online Banking Fraud, Phishing, Identity Theft.

INTRODUCTION

In the last few years, especially post demonetization in 2016 and the COVID-19 pandemic, there has been a major spike in the number of digital payments in India. Users can pay digitally using a variety of methods, including cards, wallets, mobile banking, QR codes, the Unified Payments Interface (UPI), and more. The expansion of digital transactions in India has been greatly aided by UPI.[1] However, this convenience also comes with risks, as many innocent people are misled and get scammed and lose their hard-earned money. Cyber fraud has become a major concern in the digital world, where criminals use methods such as hacking, phishing, email or spoofing, carding, vishing to steal personal data and financial information of the users. have become very common cyber crimes in the digital world. These activities often result in financial loss, identity theft, and violation of privacy rights. Though there is a rise of Internet banking services such as mobile banking, phone banking, financial transactions through debit card or credit card, electronic fund transfer the risk of cyber fraud increases significantly. As a result, ensuring digital payment security has become a major concern for regulators like the Reserve Bank of India and the government Although India has codified its first legislation on cyber crimes in the year 2000, which is the Information Technology Act, it has failed to become a strong legislation for online financial frauds.[2]

Despite the existence of cyber laws such as the Information Technology Act,2000, and RBI guidelines for digital payments security the cyber fraud still exists on a large scale thus it indicates that there are gaps in enforcement and regulatory mechanisms. Further, in order to reduce and strengthen the laws against the cyber frauds in India the Promotion and Regulation of Online Gaming Bill, 2025 was passed on 21st August 2025. This legislation is designed to encourage e-sports and social online games while imposing a complete ban on online money gaming, including their promotion, advertisements, and financial transactions

According to Cybercrime Magazine, by 2025 Cybercrime will cost the globe $ 10.5 trillion per year. Furthermore, during the next four years, worldwide cyber crime losses may increase to about 15% annually.[3] As per the annual report of the RBI, in 2022-23, 6,659 digital frauds

[1] Dr. N. Giridhar, "Digital Banking Revolution in India with Special Reference to UPI Payments", 10(11) IJSDR (Nov. 2025).
[2] Ashish Sharma & Yogender Singh, "Cyber Frauds in India's Digital Payment Ecosystem: Risk, Impacts, and Regulatory Responses", 30 Educ. Admin. Theory & Prac. 15326 (2024).
[3] Steve Morgan, Cybercrime To Cost The World $10.5 Trillion Annually By 2025, Cybercrime Magazine (Nov. 13, 2020), https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/(lasted visited May 18, 2026)

(card/internet) were reported amounting to Rs 276 crore. This is up from 3,596 fraudulent transactions worth Rs 155 crore reported in the year before. [4]

Thus the objectives of this study is to analyze the legal framework governing cyber fraud in India, to examine the effectiveness of existing regulations, to identify gaps in enforcement and reporting mechanisms, to suggest possible reforms for improving digital payment security, to understand the type of frauds on digital payments which are arising at a rapid rate and whether the prevailing legislations in India covers the emerging frauds on online transactions. This study examines India' s regulatory framework on cyber fraud and digital payment security evaluates whether current laws and guidelines are sufficient to deal with emerging cyber threats.

LITERATURE REVIEW

The books like 'Cyber Laws' by Justice Yatindra Singh, 'Cyber Laws and Information Technology' by Dr. Jyoti Rattan and Dr. Vijay Rattan. These books explain cyber laws, types of cyber crimes and laws to deal with them. They also talk about regulating digital transactions and ensuring security. The author has also referred to research articles and journals on digital payment systems and their associated risks. These studies show that with digital payments, cyber fraud like phishing and online scams has increased. Thus, there is a need for cybersecurity and user awareness. Reports from authorities like the Reserve Bank of India give important data on digital fraud. They also provide certain guidelines for digital transactions. These reports help to understand the situation of cyber fraud in India and existing regulations. The study has also referred to laws relating to cybercrimes such as The Information Technology Act, 2000, The Bharatiya Nyaya Sanhita, 2023. The author has also looked at court decisions on cyber fraud and online transactions. These legal sources help analyze the strengths and limitations of laws. However existing literature has some limitations. Most studies only focus on laws and not on practical challenges. Issues like investigation, lack of user awareness and no centralized reporting system are not discussed much. New cyber fraud techniques are also not fully covered under legal frameworks. Thus, the study tries to fill these gaps by analyzing laws and practical issues related to cyber fraud

[4] QualityKiosk Marketing, Safeguarding Banks & Financial Institutions Against Rising Digital Payment Fraud, QUALITYKIOSK (June 28, 2023), https://qualityliosk.com/blog/qualitykiosk.com/blog/qualitykiosk-technologies-safeguarding-banks-financial-institutions-against-rising-digital-payment-fraud/ (lasted visited May 18, 2026)

and digital payment security, in India. It aims to find weaknesses in the system and suggest ways to improve cyber laws and protect users better.

METHODOLOGY

Research methodology is a significant part of any study. This research is based on doctrinal and secondary research methods. The study primarily relies on doctrinal research, analyzing existing legal frameworks relating to cyber fraud and digital payment security in India. Key legislations such as the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and guidelines issued by the Reserve Bank of India have been examined in detail. This doctrinal method is suitable for legal research as it allows a detailed examination of statutory provision and regulatory guidelines which helps in understanding the structure of cyber laws and how they are applied in practice. In addition, relevant case laws and judicial precedents related to cyber fraud have been reviewed to understand how courts have addressed issues concerning digital payment security and online financial fraud. These decisions help in identifying practical challenges in enforcement of existing laws. However, no primary empirical research such as surveys or interviews has been conducted for this study.The research is based on secondary sources, including statutes, legislations, judicial decisions, journals, articles, magazines, academic research papers, government reports, and credible online sources. These sources also help in understanding recent developments in digital payment security and cyber frauds. Overall, this combination of doctrinal and secondary research methods is appropriate as it helps in systematically analyzing existing legal provisions and identifying gaps in the regulatory framework governing cyber fraud and digital payments in India**.**

MEANING OF CYBER FRAUD

Cyber Fraud is a specific type of criminal activity carried out through the use of technology, which have increased significantly over the years, causing financial losses worldwide. Cyber Fraud is a crime committed by cyber attackers through any technological devices such as computers, laptops, smartphones and the internet, with the intention of deceiving individuals and unlawfully obtaining money or sensitive information.[5] One of the common examples of

[5] Press Information Bureau, Government of India, Department of Financial Services Signs MoU with RBI Innovation Hub For Expanding and Deepening the Digital Payments Ecosystem in India, PIB (Sep. 25, 2025), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2176146&reg=3&lang=2 (lasted visited May 18, 2026)

cyber fraud is Identity theft. Stealing one's "identity," such as personal information like bank details or credit card information. Cybercriminals use various tactics to commit identity thefts such as pharming, spoofing, phishing, malvertising, and pretexting.[6]

Cyber Fraud can take various forms depending on the tactics used by the offenders, such as, account fraud, where there is an unauthorized access to the user accounts to steal data or money from the bank accounts; payment fraud, where cybercriminals steals payment details and use them to make illegal transactions, often involves card crackling and/or cardling; OTP fraud; online scams; Business Email Compromise (BEC); Ransomware etc. [7]

GROWTH OF DIGITAL PAYMENT SYSTEM

Earlier in India digital payment was not commonly used and it has been gradually developed over the years. Before, the pre-independence era Payment systems were primarily cash-based, with transactions conducted through physical currency notes and coins. Gradually in the early 1980s to 1990s there was the introduction of credit and debit cards which led to the beginning of the non cash transactions. Banks started offering card services, and Automated Teller Machines (ATMs) became commonplace which provided an alternative to cash withdrawals from bank branches. Further, in the 2000s due to the introduction of the Internet , online banking was brought into the mainstream world allowing the customers to perform banking activities such as fund transfer and bill payments. In this period there was an emergence of online shopping which provided the need for secure online payment. [8]In the 2010s digital payment grew rapidly with the widespread use of mobile phones and the launch of mobile banking apps The introduction of the UPI in 2016 has played a significant role by enabling instant and easy transactions. Digital wallets and payment platforms also became popular among users. In the 2020s due to the emergence of Covid 19 pandemic increased in the adoption of digital payments. People started using contactless payments, QR code-based transactions, and Near Field Communication (NFC) technology. Thus with the rapid growth

[6] Justice Yatindra Singh, Cyber Laws vol. 1, 6th ed. (Universal Law Publ'g 2016)
[7] SearchInform, Fraud, SEARCHINFORM, https://searchinform.com/articles/cybersecurity/cyber-threats/fraud/ (last visited May 18, 2026)
[8] Harshita Soni, The Evolution of Digital Payments in India, FINEXTRA (June 28, 2024), https://www.finextra.com/blogposting/26387/the-evolution-of-digital-payments-in-india (lasted visited May 18, 2026)

of the technology, the digital payment has also significantly increased in India which has increased the risk of cyber fraud and security concerns.[9]

REGULATIONS DEALING WITH CYBER FRAUD AND DIGITAL PAYMENT SECURITY INDIA

1. Information Technology Act, 2000

The IT Act has the legal framework for regulating cyber fraud in India. Under sections 43 and 66 of the IT Act[10], someone who willfully and illegally accesses, downloads, copies, or extracts any material or information from a computer and its related resources is subject to punishment in the form of damages and compensation. The IT Act does address identity theft specifically, but it also contains legal provisions for the unauthorized access to sensitive information and personal data. Section 66C[11]: This section describes the consequences of identity theft and indicates that they may include sentence of up to three years in jail or fine upto one lakh rupees. Section 66D[12]: This section outlines the consequences for utilizing a computer resource to impersonate another person in order to commit fraud. These include a maximum penalty of three years in jail, a maximum fine of one lakh rupees, or both. The two pieces of legislation discussed about identity theft and other online frauds connected to ATMs are the IT Act and the IT (Amendment) Act of 2008.

2. Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023 also plays an important role in addressing cyber fraud. Data theft under section 43(b) is read with Section 66 of the IT Act is associated with section 303(2), 318(4) of BNS, hacking under section 43(a) read with Section 66C of IT Act is associated with section 303(2) BNS, credit card fraud under section 43(a), 43(b) read with section 66 of IT Act is associated with section 318(4), 337, 338, 340(2), 342 BNS, dishonestly receiving stolen computer resources or communication device under section 66B is associated with section 317(4), 317(5) of BNS, phishing under section 43 of the IT Act is associated with section 303(2), 318(4) of BNS, embezzlement, that is diverting money to

[9] Mrs. Jinya Khurshid Katrak, "Evolution of Digital Payment System in India: A Review", 9(3) INT'LJ. SOC. IMPACT (2024) .
[10] Information Technology Act, Sections 43 & 66, 2000 (India)
[11] Information Technology Act, Section 66C, 2000 (India)
[12] Information Technology Act, Section 66D, 2000 (India)

one's own account is explained under criminal breach of trust, misappropriation of property under the Bharatiya Nyaya Sanhita, 2023.[13]

3. **Payment and Settlement System Act, 2007**

The Payment and Settlement System Act, 2017[14] provides a legal framework for regulating electronic payment systems in India. The Acts give power to the Reserve Bank of India in order to supervise and control payment system operators so that financial transactions remain safe and efficient. According to this Act, the entity's operating payment system must obtain authorization from the RBI before commencing operations. This regulatory mechanism ensures that digital payment service providers comply with prescribed security standards and operational guidelines.

4. **The Digital Personal Data Protection Act of 2023 (DPDP)**

The Digital Personal Data Protection Act (DPDP) was enacted by the Central Government of India on August 11, 2023 to protect the individual personal data such as Aadharcard, phone numbers, emails, biometric and other important documents and regulate how organizations collect, use and process such data. The Act provides that the organizations must obtain explicit consent from individuals before collecting or processing their data. The Act imposes several obligations for data fiduciaries, such as data minimization (collecting only necessary information), storage limitation (retaining data only as long as required), and data breach notification (information users and authorities in case of a security breach). All these measures aim to reduce the risk of data misuse and enhance transparency.[15]

ROLE OF RESERVE BANK OF INDIA IN DIGITAL PAYMENT SECURITY

RBI ensures that individuals are safeguarded against fraud, unauthorized transactions, and unfair practices. RBI has also introduced secure digital payment security measures. These are

1. RBI provides security measures for digital payment platforms, including encryption standards, secure authentication protocols, and transaction monitoring systems to detect and prevent cyber fraud.

[13] Bharatiya Nyaya Sanhita, 2023 (India).
[14] The Payment and Settlement Systems Act, No. 51 of 2007, Preamble (India Code).
[15] Ashish Sharma & Yogender Singh, "Cyber Frauds in India's Digital Payment Ecosystem: Risk, Impacts, and Regulatory Responses," 30 Educational Administration: Theory and Practice 15326 (2024).

2. RBI provides a fair mechanism for resolving disputes related to digital transactions, ensuring timely redressal of grievances and fair treatment of consumers who are facing issues relating to the online payment.[16]

3. RBI conducts public awareness campaigns and educational programs to educate people to safely use digital payment practices, cybersecurity tips, and responsibilities while using digital payment services.

4. OTP is required for adding new payees because it is risky and the process is much more secure.

5. In case of High value transactions the risk is higher thus an OTP is required so that extra security is there for important transactions. The OTP only works for a limited time so that there is less chance of misuse.[17]

7. Technologies like digital signatures and authentication codes (such as KMAC) are used to verify transactions and prevent unauthorized activities.

8. Alerts are sent to the customer through email or SMS for the certain transactions so that they are immediately aware of any suspicious activity. [18]

ISSUES AND CHALLENGES

1. Lack of usability

Digital payment systems are difficult to use as they require the users to provide a lot of personal information, making the process complicated and also having a risk of cyber fraud.

2. Issue with e-cash

E-cash is not acceptable everywhere because its use is limited. Thus, both the parties should have an account in the same bank account that provides e-cash.

[16] Vasundhara Shankhar & Aastha Arora, RBI's Guidelines for Digital Payment Companies- An Analysis, LiveLaw (July 15, 2021), https://www.livelaw.in/amp/law-firm-articles-/reserve-bank-of-india-guidelines-digital-payment-companies-177499 (lasted visited May 18, 2026)
[17] Reserve Bank of India. Mobile Banking Transactions in India, RBI (Feb. 10, 2015), https://www.rbi.org.in/commonman/english/scripts/PressRelease.aspx?Id=3232 (lasted visited May 18, 2026)
[18] Reserve Bank of India, Security and Risk Mitigation Measures for Electronic Payment Transactions, RBI (Feb. 18, 2009), https://www.rbi.org.in/commonman/English/Scripts/Notification.aspx?Id=2336 (lasted visited May 18, 2026)

3. Lack of security

There is a risk of data theft and financial information in the digital payment system as it is accessible targets for the hackers to steal money and any other personal information.

4. Lack of trust

Digital payment has a history of cyber fraud, identity theft, phishing etc. Thus many users do not trust digital payments system due to the fear of fraud and data being misused

5. Lack of awareness

Digital payment system is a difficult task even well educated people have difficulty paying online due to the lack of knowledge about how to use online payment, which technically leads them to avoid it

6. Online Payments Are Not Suitable in Rural Areas:

Due to the low literacy rate, those that are literate are unable to use computers or mobile phones. They are not interested in online payment since they are uninformed of technical advances. As a result, locals cannot use an online payment method. [19]

7. Highly Expensive and more Time Consuming:

Digital payment systems can be more expensive and sometimes time-consuming as it involves set costs, machine expenses, administrative costs.[20]

8. Technical error/ System failure

The digital payment system becomes difficult due to technical glitches when the bank has a server down, the payment gets struck and money is deducted but not received.[21]

9. Poor internet connectivity

[19] M. Reddi Naik & K. Sridevi, Issues and Challenges of Electronic Payment Systems, ResearchGate (2024), https://www.researchgate.net/publication/384546714_ISSUES_AND_CHALLENGES_OF_ELECTRONIC_PAYMENT_SYSTEMS. (lasted visited May 18, 2026)

[20] Philip Thomas, Effects of Digital Payment Transaction Costs on Customer Satisfaction and sales Performance in Tesco Supermarket, ResearchGate (2024), https://www.researchgate.net/publication/404689190_Effects_of_Digital_Payment_Transaction_Costs_on_Customer_Satisfaction_Sales_Performance_in_Tesco_Supermarket (lasted visited May 18, 2026)

[21] Paytm, What Happens if Your Bank Server is Down?, Paytm Blog, https://paytm.com/blog/payments/upi/what-happens-if-your-bank-server-is-down/ (last visited May 18, 2026).

A good internet connection is required for digital transactions. Thus these transactions become difficult due in remote or rural areas because of poor internet connections.[22]

10. Fraud through phishing/scams

A secure system also sometimes fails due to human error because users are tricked by hackers who ask for fake links or calls asking for OTP.

11. Lack of grievance redressal awareness

Another issue is lack of awareness regarding grievance redressal mechanisms. People are not aware about where and how to file a complaint regarding digital issues. Due to this they delay reporting fraud on time which makes it difficult to take action.[23]

JUDICIAL APPROACH TOWARDS DIGITAL PAYMENT FRAUD

- **State Bank of India v. Pallabh Bhowmick & Ors. (2025)[24]**

In this case, the respondent became a victim of online banking fraud after installing a remote access app. There were three unauthorized online transactions totaling ₹94,204.80 from the respondent's bank account. The respondent immediately informed the bank and the police. Despite timely reporting, the bank failed to reverse the transaction or provide recovery measures.

Further, The Supreme Court upheld Gauhati High Court ruling and held SBI fully liable for the fraudulent withdrawal. The bank was directed to refund the entire amount to the customer. This judgment emphasized stronger Consumer Protection, it maintains robust cybersecurity mechanisms and monitoring systems, it recognizes the Digital Banking Risks. The ruling also serves as an important precedent for disputes involving online banking fraud.

- **Amazon Seller Services Pvt. Ltd. v. Amazonbuys.in & Ors. (Delhi High Court)[25]**

[22] Joydeep Mukherjee et al., Digital Banking and Financial Inclusion in Rural Economies, ResearchGate (Jan. 2025),https://www.researchgate.net/publication/388326365_Digital_Banking_and_Financial_Inclusion_in_Rural_Economies (lasted visited May 18, 2026)
[23] Rising digital frauds, mounting consumer grievances a growing concern for banks, RBI says, The Economic Times (Dec. 2025), https://meconomictimes.com/industry/banking/finance/bank/rising-digital-frauds-mounting-consumer-grievances-a-growing-concern-for-banks-rbi-says/articleshow/126232321.cms (lasted visited May 18, 2026)
[24] State Bank of India v. Pallabh Bhowmick & Ors, 2025 INSC 102
[25] Amazon Seller Services Pvt. Ltd. & Anr. v. Amazonbuys.in & Ors., CS (COMM) 364/2022, 2025:DHC:1104

In this case, fake websites like "Amazonbuys.in" misused Amazon's name and logo to cheat users by offering false seller registrations and collecting money. The Delhi High Court held that this amounted to trademark and copyright infringement, passing off, and digital fraud. It found that the defendants were misleading consumers by impersonating Amazon. The case is important as it shows how courts deal with online impersonation and protect consumers from digital fraud.

SUGGESTIONS

As cyber fraud is taking place day by day the users should take careful steps to protect their personal and financial data while making online transactions, personal details like OTP, PIN, CVV, passwords, and bank information should never be shared with anyone. People should avoid clicking on unknown or suspicious links received through emails or messages. People should avoid downloading Unverified or unofficial applications as they may contain malware.

People should avoid the use of Public Wi-Fi networks for financial transactions because they increase the risk of hacking. Users should enable two-factor authentication for added security. Before using any application, its authenticity should be verified, and unnecessary app permissions should be disabled after installation.

The user should regularly monitor the account activity, such as checking last login details, is important. In case of fraud, victims should immediately lodge an FIR or General Diary to help recover funds. There is also a need for greater public awareness and stronger enforcement of cyber laws to protect digital users.

DISCUSSIONS

This study examines the legal framework governing cyber fraud and digital payment security in India. The analysis shows that though India has enacted strong laws and regulatory measures the cyber fraud took place rapidly in India due to the enforcement gaps and technological challenges. The Government of India has enacted several Acts, such as Information Technology Act 2000, Bharatiya Nayaya Sanhita 2023, and Reserve Bank of India guidelines in order to protect from cyber frauds. Despite the enforcement of these laws, their effectiveness is limited. Delayed investigation and slow recovery of stolen funds in case

of cyber fraud are the main reasons which reduces public trust in digital payment systems. The findings indicate RBI should introduce real-time fraud monitoring systems to reduce unauthorized transactions. Further in order to protect the people from fraud the bank should use advanced fraud detection tools to identify suspicious transactions and the users should be educated regarding cyber fraud techniques such as phishing, OTP Scams, fake customer care calls etc. Thus, due to lack of knowledge about the cyber frauds techniques, awareness campaign and public education are to be conducted to reduce cyber frauds The legal framework such as IT Act,2000; BNS 2023; and RBI guidelines on digital payments security provides a strong foundation.However, the existing legal framework has certain drawbacks, such as the provisions do not fully include all types of modern cyber fraud. In addition to this, the absence of a fully centralized reporting system for cybercrime complaints often leads to delays and inefficiency. Due to the increasing number of Cyber fraud, it is recommended that India should develop a unified cyber fraud reporting platform to ensure quicker resolution of cases. India should also introduce stricter punishment in cases of digital impersonation and stronger compensation mechanism in cases of cyber fraud. Though India has implemented several digital payments regulations in recent years, continuous reforms are still required to deal with new types of cyber fraud and protect the users effectively.

CONCLUSION

The present research discusses cybercrime and fraud in digital payment systems. Due to the increase of digitalization, the majority of transactions are being used online. Although this has made payments quicker and more convenient, it has also made the risk of cyber fraud greater. Cybercrime in the form of phishing, identity theft, online scams etc. have increased, forcing us to implement adequate cybersecurity measures to eradicate such threats. Further, cyber fraud and Digital Payment Security are growing concerns in India owing to the fast expansion of digital transactions. The study has examined the existing legal framework, such as the Information Technology Act of 2000, Bharatiya Nyaya Sanhita of 2023 and guidelines issued by the Reserve Bank of India. These laws form the foundation for cyber fraud regulation and digital payment security. Although these laws exist, cyber fraud is still increasing. Although laws exist, cyber fraud is still increasing. There are several issues in dealing with cyber fraud, such as delay in investigation, lack of awareness among people about how fraud takes place, and absence of proper safety measures. There are also certain enforcement gaps in the existing laws. Therefore, there is a need for improvement in

enforcement and greater awareness among the public. People should be made aware of different types of cyber fraud such as phishing, OTP scams, and fake calls and how to protect themselves. In addition, stronger laws should be imposed to control cyber fraud, and there should be better monitoring of digital transactions and security systems

Overall, while India has made significant progress in regulating digital payment systems, continuous reforms and stronger implementation of existing laws are necessary to effectively address the evolving nature of cyber fraud and to ensure better protection of users.