IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, May 2026
Impact Factor: 8.2

Cyber Fraud in Online Trading: A Critical Analysis of Regulatory Frameworks and Investigative Challenges in India

Deep Dubey and Dr. Ram Kumar Sahu
2nd Year Law Student at Amity University Raipur, Chhattisgarh, India
Assistant Professor at Amity University Raipur, Chhattisgarh, India

Abstract: *The rapid digitalization of the Indian financial sector has led to an exponential increase in online trading, which has simultaneously exposed investors to sophisticated cyber-fraud mechanisms In 2020 alone, India reported approximately 1.16 million cyberattack cases, reflecting a growing vulnerability in the digital economy This research provides a critical analysis of the current regulatory frameworks, primarily governed by the Information Technology Act of 2000 and the Securities and Exchange Board of India guidelines, to assess their effectiveness in protecting retail investors .The study identifies significant investigative hurdles, including jurisdictional complexities, an overlap between the Indian Penal Code and the IT Act, and a shortage of technical expertise within law enforcement agencies . By evaluating recent stockbroking frauds and enforcement lapses, the paper concludes with policy recommendations aimed at strengthening judicial procedures and enhancing technological capabilities for fraud detection.*

Keywords: *digitalization*

I. INTRODUCTION

The Indian stock market has undergone a paradigm shift from traditional physical trading to high-frequency online platforms, driven by affordable mobile computing and reduced bandwidth costs (Bhanawat & Khang, 2024; Sıngh et al., 2023). While this digitalization has democratized access to wealth creation, the "not secure by design" nature of internet infrastructure has invited an unprecedented rise in dubious practices by fraudulent entities and unscrupulous stockbrokers (Kandukuri, 2023; Sıngh et al., 2023). Today, online trading platforms face severe impediments such as data theft, identity personation, and phishing, which threaten the reliability of capital markets (Kashyap & Chaudhary, 2023; Singh & Gautam, 2022).

In India, the primary legislation governing these digital offenses is the Information Technology Act of 2000, supported by the regulatory oversight of SEBI (Manjunath & S, 2024; S., 2023). However, as the modi operandi of cybercriminals evolve, the existing legal system faces a "regulatory gap," where enforcement often lags behind technological advancements (Kandukuri, 2023). For instance, while Section 66 of the IT Act addresses hacking and data theft, the cross-border nature of these crimes often makes traditional jurisdictional boundaries obsolete (Elavarasi & Elango, 2017; Singh & Gautam, 2022). Protecting the interests of the 21st-century digital investor now requires a multidisciplinary approach that combines legal reform with advanced cyber forensics (Elavarasi & Elango, 2017; Manjunath & S, 2024).

II. PROBLEM STATEMENT

Despite the implementation of the IT Act and specialized SEBI regulations, online trading fraud in India continues to rise, with an average of over 3,000 cybersecurity issues reported daily The core problem lies in a fragmented regulatory landscape where overlapping provisions between the IPC and the IT Act create legal inconsistencies

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/IJARSCT-34739

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, May 2026 Impact Factor: 8.2

regarding bailable and non-bailable offenses Furthermore, investigative agencies often lack the specialized technical training and forensic labs required to preserve digital evidence from decentralized or extraterritorial servers This gap between the volume of digital transactions and the capacity of the legal system to punish offenders undermines investor confidence and poses a systemic risk to India's financial stability.

III. RESEARCH OBJECTIVES

The primary objectives of this study are:

- To analyze current trends in cyber fraud within the Indian online trading ecosystem, focusing on the most common modi operandi used to defraud investors
- To evaluate the effectiveness of the legal framework, specifically the IT Act 2000 and SEBI's corrective regulations, in detecting and preventing fraudulent activitie
- To identify investigative and judicial challenges, such as jurisdictional hurdles, overlapping legal provisions, and the shortage of technical experts in cybercrime units.

IV. RESEARCH METHODOLOGY

4.1 Research Design

This study adopts a multi-dimensional research design comprising Descriptive, Analytical, and Doctrinal methodologies to ensure a comprehensive investigation of cyber fraud in Indian online trading.

4.2 Descriptive Design

Utilized to outline the current landscape of cybercrime in India, documenting the exponential rise in cases reaching over 1.16 million reported incidents in recent years and the evolving nature of digital trading platforms

4.3 Analytical Design

Applied to evaluate the correlation between the digitalization of financial services and the increasing complexity of stockbroking frauds This approach allows for the critical examination of why existing investigative mechanisms often fail to curb fraudulent activities despite the presence of regulatory bodies

4.4 Doctrinal Design

Focused on the "law as it is" by analyzing statutes such as the Information Technology Act, 2000, and the Indian Penal Code. This method is essential for identifying the legal inconsistencies and "regulatory gaps" that hinder effective prosecution in the financial sector.

V. DATA SOURCES

The research relies on a combination of secondary data sources to ensure high reliability and validity of the findings:

National Crime Records Bureau & MHA

These provide the official statistical foundation for analyzing the volume and types of cybercrimes reported across various Indian jurisdictions.

SEBI Annual Reports and Circulars

Essential for tracking regulatory actions taken against fraudulent stockbrokers and understanding the evolution of compliance requirements for online trading platforms.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, May 2026
Impact Factor: 8.2

RBI Fraud Reports

Used to capture the broader financial impact of digital frauds and the systemic risks they pose to the Indian banking and investment ecosystem.

Research Journals and Case Studies

Peer-reviewed academic literature and documented legal cases (such as those involving stockbroking enforcement) provide the necessary context to interpret investigative challenges and institutional failures.

VI. TOOLS & TECHNIQUES

To process the collected data and legal statutes, the following tools and techniques are employed:

Legal Analysis

This is the primary tool used to scrutinize the overlapping provisions between the IT Act and traditional criminal laws. It aims to highlight the procedural difficulties in adjudicating bailable versus non-bailable cyber offenses in India.

Content Analysis

Systematically applied to review SEBI's regulatory circulars and legislative amendments to determine whether the "regulatory framework" has kept pace with technological advancements in online trading.

Comparative Analysis

Employed to benchmark Indian cyber-security laws against international standards, identifying specific institutional and operational challenges such as the lack of specialized forensic labs and technical expertise that delay the reporting and investigation of financial crimes.

VII. TRENDS IN CYBER FRAUD IN ONLINE TRADING

7.1 Growth of Online Trading

The Indian financial landscape has witnessed a paradigm shift from traditional physical trading to high-frequency online platforms, a transition accelerated by the post-COVID-19 digitalization wave This growth is primarily driven by:

7.2 Increase in Demat Accounts

The ease of opening digital accounts and the influx of retail investors during the pandemic led to an unprecedented surge in market participation. However, this "digitalization of finance" has outpaced the general public's awareness of cybersecurity protocols

7.3 Rise of Mobile Trading Apps

Affordable mobile computing and reduced bandwidth costs have made trading accessible to a broader demographic. While these apps offer convenience, many are "not secure by design," creating vulnerabilities that cybercriminals exploit to gain unauthorized access to investor portfolios

VIII. RISE IN CYBER FRAUD CASES

With the democratization of trading, the frequency and scale of financial cyber-offenses have escalated significantly.

8.1 Statistical Growth

India reported approximately 1.16 million cyberattack cases in 2020 alone, highlighting a systemic vulnerability in the digital economy. Reports suggest that over 3,000 cybersecurity issues are now encountered daily, many targeting the financial and stockbroking sectors.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, May 2026
Impact Factor: 8.2

8.2 Investor Losses

The "supervision gap" in digital platforms has resulted in significant financial losses for retail investors. This trend is not merely anecdotal; analysis of stockbroking frauds reveals that unscrupulous entities leverage the anonymity of the internet to commit large-scale misappropriation of funds before regulatory bodies can intervene.

IX. COMMON TYPES OF FRAUD

The *modus operandi* of cyber-fraudsters in the Indian trading sector has become increasingly sophisticated, often bypassing traditional security measures:

9.1 Fake Trading Apps

Fraudsters develop counterfeit mobile applications that mirror legitimate trading platforms. These apps entice investors with promises of high returns, only to vanish once significant capital has been deposited .

9.2 Telegram/WhatsApp "Pump & Dump" Schemes

Social media platforms have become hubs for market manipulation. Fraudsters use these channels to artificially inflate (pump) the price of a stock through coordinated misinformation and then sell off (dump) their shares, leaving retail investors with worthless assets.

9.3 Phishing and Impersonation

Cybercriminals use deceptive links to steal login credentials or impersonate SEBI-registered brokers to gain trust . These phishing attacks are often the first step in "identity personation" crimes, where the fraudster takes full control of the victim's digital trading account.

X. REGULATORY FRAMEWORK IN INDIA

10.1 Key Regulatory Bodies

The governance of online trading in India is managed by a multi-institutional framework designed to ensure market integrity and technical security:

10.1.1 Securities and Exchange Board of India

As the primary regulator of the capital markets, SEBI is responsible for protecting the interests of retail investors and regulating the conduct of market intermediaries such as stockbrokers and clearing corporations.

10.1.2 Reserve Bank of India

The RBI oversees the digital payment gateways and financial transactions that facilitate online trading, ensuring that the underlying monetary infrastructure is resilient against cyber frauds.

10.1.3 Ministry of Electronics and Information Technology

This ministry formulates broad national policies for the digital economy and manages the Indian Computer Emergency Response Team, which tracks and responds to large-scale cybersecurity incidents.

10.2 Key Legal Provisions

The prosecution and regulation of cyber fraud in trading are governed by a combination of general criminal law and specialized statutes:

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, May 2026 Impact Factor: 8.2

Information Technology Act, 2000
This is the cornerstone of India's cyber law. Sections 43 and 66 are frequently invoked to address unauthorized access to computer systems, data theft, and hacking within trading platforms.

IPC Provisions Related to Fraud
While the IT Act is specialized, the Indian Penal Code remains critical for addressing the fraudulent intent. Sections 420 (cheating), 406 (criminal breach of trust), and 468 (forgery for the purpose of cheating) are often applied in tandem with the IT Act to secure convictions in stockbroking frauds.

SEBI Regulations
These guidelines mandate strict compliance for digital conduct, requiring intermediaries to maintain high standards of transparency and preventing "unauthorized trading" through mandatory verification of client instructions.

10.3 SEBI Initiatives
To stay ahead of evolving digital threats, SEBI has launched several targeted initiatives aimed at system resilience and investor protection:

10.3.1 Cyber Security and Cyber Resilience Framework
SEBI mandates that all stockbrokers and depository participants adhere to a robust framework for identifying, protecting, and recovering from cyber-attacks. This includes mandatory periodic audits and the implementation of multi-factor authentication for trading accounts.

10.3.2 SCORES Grievance Redressal System
The SEBI Complaints Redress System is a centralized, web-based platform that allows investors to lodge and track grievances against market intermediaries. While it provides a formal channel for resolution, studies indicate that the speed of redressal remains a concern for retail investors.

10.3.3 Investor Awareness Campaigns
SEBI facilitates extensive education programs to inform the public about the risks of "pump and dump" schemes on social media and the dangers of using unregistered trading applications

XI. CRITICAL ANALYSIS OF REGULATORY EFFECTIVENESS

11.1 Strengths
The Indian regulatory landscape for online trading is built upon a strong institutional framework led by SEBI, which has successfully transitioned the market from physical to digital settlement A key strength lies in the mandatory compliance protocols for intermediaries; SEBI's "Cyber Security and Cyber Resilience Framework" ensures that registered brokers maintain audited digital infrastructures Furthermore, the government has increased digital surveillance mechanisms through the Indian Computer Emergency Response Team, providing a centralized layer of threat intelligence for the financial sector.

11.2 Weaknesses
Despite these strengths, there is a noticeable delayed regulatory response to emerging fraud techniques like "pump and dump" schemes on encrypted messaging apps, which often cause mass investor loss before intervention occurs The current system suffers from a lack of real-time monitoring of unregulated social media channels that influence market sentiment Additionally, there is weak enforcement regarding unregulated apps; many fraudulent trading platforms

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, May 2026 Impact Factor: 8.2

operate in a legal grey zone where SEBI's jurisdictional reach is limited until a formal complaint is lodged through SCORES.

11.3 Gap Identified: Reactive vs. Proactive

The fundamental gap in the current framework is that regulation remains reactive rather than proactive. Investigative actions and circulars are typically released *after* a new type of fraud has already victimized thousands of retail investors There is an urgent need for a "pre-emptive" regulatory stance that utilizes AI-driven surveillance to flag suspicious trading patterns before they manifest as large-scale scams.

XII. INVESTIGATIVE CHALLENGES IN INDIA

12.1 Technological Challenges

Fraudsters increasingly use **encryption and anonymization tools** to mask their identities, making it difficult for agencies to link a digital crime to a physical suspect The widespread use of **VPNs and offshore servers** allows criminals to host fraudulent trading sites in jurisdictions where Indian law enforcement has no direct authority, complicating the digital trail and evidence preservation process.

12.2 Jurisdictional Issues

Cyber-fraud in trading is rarely localized; it often involves cross-border fraud networks where the perpetrator, the server, and the victim are in different countries. This creates immense difficulty in international cooperation, as the process of Mutual Legal Assistance Treaties is often too slow to prevent the rapid movement of stolen funds across international digital wallets.

12.3 Institutional Challenges

There is a critical shortage of cyber forensic experts within state police departments, leading to a backlog of electronic evidence that needs analysis . Furthermore, the limited training of frontline police personnel often results in a "digital literacy gap," where officers struggle to understand the complexities of algorithmic trading or blockchain-based transactions during the initial reporting phase.

12.4 Operational Challenges

Operational hurdles significantly impede justice for retail investors. There is a frequent delay in FIR registration, as police stations often struggle to determine if a case is "civil" (trading loss) or "criminal" (fraud) This delay leads to a low recovery of funds, as stolen capital is moved through layers of "mule accounts" within minutes Finally, complex evidence collection requirements under the Indian Evidence Act such as Section 65B certificates for electronic records often lead to the dismissal of cases due to procedural technicalities.

XIII. COMPARATIVE PERSPECTIVE

While India's regulatory framework is evolving, comparing it with global standards reveals critical gaps in proactive enforcement. International research highlights that while countries like the USA and UK emphasize high-frequency monitoring and operational resilience, India's current mechanism faces significant "jurisdictional hurdles" and procedural delays in international cooperation. Unlike models that prioritize "security by design," the Indian digital trading landscape often deals with "regulatory gaps" where technology—such as VPNs and offshore servers—is used to bypass local enforcement Strengthening the Indian framework requires moving toward the transparency standards seen in more mature digital economies, where information disclosure and cybersecurity policies are more tightly integrated into the financial market's core.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, May 2026
Impact Factor: 8.2

XIV. DISCUSSION OF FINDINGS

14.1 Persistent Growth of Fraud

Despite the implementation of the Information Technology Act and SEBI guidelines, the volume of cyber fraud continues to escalate, largely driven by the rapid "digitalization post-COVID" and the influx of retail investors who lack adequate digital literacy.

14.2 The Enforcement Lag

A major finding is the systemic delay in the investigation process. Research indicates that the lack of specialized "cyber forensic experts" and technical training within police departments leads to critical delays in evidence collection and FIR registration.

14.3 Technological Asymmetry

Technology is evolving faster than legal responses. Fraudsters are leveraging encrypted tools and "not secure by design" mobile apps to commit stockbroking frauds, while the legal system remains encumbered by overlapping provisions between the IT Act and the IPC.

14.4 Inadequate Investor Protection

The study identifies that investor grievances, often lodged through systems like SCORES, face resolution challenges due to the sheer volume of cases and the complexity of digital evidence required to prove fraudulent intent.

XV. CONCLUSION

India has established a foundational regulatory framework to address cyber fraud in online trading. However, this study concludes that the effectiveness of these measures is severely hampered by reactive enforcement, a shortage of technical expertise, and operational challenges in cross-border investigations. The "regulatory gap" between the volume of digital transactions and the capacity for judicial adjudication poses a significant risk to market integrity. A transition from reactive gatekeeping to a proactive, technology-driven surveillance model is essential to restore and maintain investor confidence in India's digital economy.

XVI. RECOMMENDATIONS

16.1 Policy Recommendations

16.1.1 Proactive Regulatory Stance

Regulatory bodies should shift from reactive circulars to proactive, real-time surveillance of digital platforms to identify "pump and dump" patterns before they cause systemic damage.

16.1.2 Legal Harmonization

There is an urgent need to resolve the legal inconsistencies between the IT Act and the IPC to streamline the adjudication of cyber-financial crimes.

16.2 Technological Recommendations

16.2.1 Advanced Analytics

Financial institutions and regulators should adopt predictive analytics and "complex network" monitoring similar to models being explored in the insurance sector—to detect fraudulent claim patterns and market manipulation.

16.2.2 Traceability Tools

The integration of blockchain for transaction logging should be explored to ensure an immutable audit trail, making it difficult for fraudsters to hide digital footprints across multiple accounts.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, May 2026
Impact Factor: 8.2

16.3 Institutional Recommendations

16.3.1 Specialized Cyber Units

Government agencies must prioritize the establishment of dedicated cybercrime investigation units staffed by trained forensic experts to reduce the current backlog of cases.

16.3.2 Inter-agency Coordination

Improve real-time data sharing between the RBI, SEBI, and law enforcement to facilitate the "fast freezing" of funds in reported fraud cases.

16.4 Investor Awareness

16.4.1 Digital Literacy

Educational programs must go beyond basic financial literacy to include "cyber hygiene," specifically targeting the detection of phishing links and fraudulent mobile applications.

Limitations

This study is primarily limited by its dependence on published secondary data from the NCRB and regulatory reports, which may not capture the most recent, undocumented "modi operandi" of cybercriminals. Furthermore, the significant "underreporting" of cyber fraud in India due to procedural complexities likely means the true scale of financial loss is higher than officially documented.

Future Scope

Future research should focus on the impact of emerging technologies, such as the use of Artificial Intelligence in both committing and detecting financial fraud. Further investigation is needed into the "supervision gap" within decentralized finance and how algorithmic trading platforms can be secured against increasingly sophisticated personation and data theft crimes.

REFERENCES

[1]. Bhanawat, H., & Khang, A. (2024). An Examination of Data Protection and Cyber Frauds in the Financial Sector. In Auerbach Publications eBooks (p. 345). https://doi.org/10.1201/9781032618845-19

[2]. Bhatia, D. (2022). A Comprehensive Review on the Cyber Security Methods in Indian Organisation. International Journal of Advances in Soft Computing and Its Applications, 14(1), 103. https://doi.org/10.15849/ijasca.220328.08

[3]. Brahmaiah, B. (2018a). Arbitration on Margin Positions Liquidation at Stock Exchange in India. Theoretical Economics Letters, 8(10), 1701. https://doi.org/10.4236/tel.2018.810110

[4]. Brahmaiah, B. (2018b). Arbitration on Unauthorized Trading by the Trading Member of Indian Stock Exchange: An Empirical Study. Theoretical Economics Letters, 8(14), 2914. https://doi.org/10.4236/tel.2018.814182

[5]. Cosma, S., & Rimo, G. (2024). Redefining insurance through technology: Achievements and perspectives in Insurtech. Research in International Business and Finance, 70, 102301. https://doi.org/10.1016/j.ribaf.2024.102301

[6]. Elavarasi, M., & Elango, N. M. (2017). Analysis of Cybercrime Investigation Mechanism in India. Indian Journal of Science and Technology, 10(40), 1. https://doi.org/10.17485/ijst/2017/v10i40/119416

[7]. Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? The Journal of Risk Finance, 17(5), 474. https://doi.org/10.1108/jrf-09-2016-0122

[8]. Kandukuri, R. (2023). An analysis of stockbroking frauds and regulatory action in India. Journal of Financial Crime, 31(4), 1037. https://doi.org/10.1108/jfc-04-2023-0076

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, May 2026
Impact Factor: 8.2

[9]. Kashyap, A. K., & Chaudhary, M. Z. (2023). Cyber security laws and safety in e-commerce in India. Law and Safety, 89(2), 207. https://doi.org/10.32631/pb.2023.2.19

[10]. Kaur, J. (2018). Investors' probable solutions to their problems: a study of Punjab. International Journal of Law and Management, 60(2), 355. https://doi.org/10.1108/ijlma-11-2016-0138

[11]. Kuzior, A., Zakharkina, L. S., Kubaščíková, Z., Chentsov, V., & Lyeonov, S. (2023). Insurance market transparency research trends: Bibliometric analysis. Insurance Markets and Companies, 14(1), 136. https://doi.org/10.21511/ins.14(1).2023.12

[12]. Manjunath, M., & S, D. S. (2024). A Study on Cyber Frauds Post Digitalization in India. International Journal for Research in Applied Science and Engineering Technology, 12(4), 1790. https://doi.org/10.22214/ijraset.2024.60191

[13]. Rani, K. (2023). Cybercrime and Legal Responses in the Indian Jurisdiction. Indian Journal of Law., 1(1), 35. https://doi.org/10.36676/ijl.2023-v1i1-05

[14]. S., A. A. K. R. (2023). State of the Art - Cybercrimes and Cyber Security Policies and Countermeasures. International Journal for Research in Applied Science and Engineering Technology, 11(11), 2744. https://doi.org/10.22214/ijraset.2023.57092

[15]. Singh, V., & Gautam, D. R. (2022). Cyber Crime, Security and Regulation in India (p. 147). https://doi.org/10.55662/book.2022ccrs.005

[16]. Sıngh, V., Malik, V., & Mittal, R. (2023). Challenges to Cybercrime Reporting, Investigation, and Adjudication in India. In Apple Academic Press eBooks (p. 1). https://doi.org/10.1201/9781003369479-1

[17]. Zappa, D., Clemente, G. P., Corte, F. D., & Savelli, N. (2023). Editorial on the Special Issue on Insurance: complexity, risks and its connection with social sciences. Quality & Quantity, 57, 125. https://doi.org/10.1007/s11135-023-01705-9