International Journal of Commerce and Management Studies (IJCAMS)
ISSN 2456-3684, Vol 10, No 2,2025
www.ijcams.com

# E-Banking Frauds: Insights from Literature and Security Innovations

**Vivek Kumar Sindhi #1, Ritika Maini *2, Dr. Harsimran Kaur #3**

**#1 Assistant Professor, PG Dept of Commerce, Govt. Bikram College of Commerce, Patiala (Punjab)**
viveksindhi29@gmail.com

***2 Assistant Professor, Dept of Computer Science, Govt. Bikram College of Commerce, Patiala (Punjab)**
maini_ritika@rediffmail.com

**#3 Assistant Professor, Dept of Computer Science, Govt. Bikram College of Commerce, Patiala (Punjab)**
harsimranmahajan1980@gmail.com

**Abstract:** The world economy has been impacted by the rapid development of digital technologies, which have been fundamentally altered the people and businesses. This digital revolution has also led to an increase in financial fraud and online scams, posing major hazards to people, organizations, and financial institutions. This article examines how financial crimes and internet scams have evolved in the digital age. In particular, it looks at prevalent tactics such as social engineering attacks, cryptocurrency scams, online payment fraud, phishing, and identity theft. The study explores the methods employed by cybercriminals, examines the technological and psychological vulnerabilities that expose victims, and analyzes the broader societal impact of these fraudulent activities. It also emphasizes how crucial laws, cybersecurity developments, and public awareness are to the battle against online fraud. This article provides a knowledge of the difficulties posed by financial frauds and internet scams. It also suggests practical ways to mitigate the effects of these crimes in our increasingly linked society.

**Keywords:** Communication; Cybercriminals; Innovations; Swindling; Blockchain; The Internet of Things (IoT)

## 1.Introduction:

The digital age has revolutionized the way individuals, organizations, and governments operate, offering unprecedented levels of convenience and connectivity. The internet, smart devices, and cloud computing have made communication, shopping, and banking more accessible and convenient than ever before [1–3]. A typical internet shopping system is shown in Figure 1.
The digital revolution, despite its advantages, has simultaneously streamlined the proliferation of financial crime and internet fraud. As technology has advanced, cybercriminals have devised increasingly sophisticated methods to exploit both human vulnerabilities and weaknesses in digital systems [4, 5].


**Figure 1: Digital Fraud**

### 1.1 The Evolving Threat of Digital Fraud

Online scams and financial fraud broadly encompass illicit activities such as ransomware, cryptocurrency scams, identity theft, and phishing. These pervasive crimes inflict substantial financial and psychological harm on individuals, small businesses, and large corporations. The scale of such operations in India is alarming; according to RBI and cybersecurity reports, digital fraud has resulted in losses of thousands of crores annually, with many incidents remaining unreported or unresolved. One important characteristic of online and financial fraud is they're constantly changing and adaptable in nature [6,7]. Hackers are constantly upgrading their tactics by leveraging emerging technologies like artificial intelligence (AI), blockchain, and the Internet of Things (IoT), making their schemes increasingly complex and deceptive [8]. At the same time, the global nature of the internet poses significant challenges for Indian law enforcement agencies in tracing and prosecuting cybercriminals, especially when operations span multiple jurisdictions. Our increasing dependency on digital devices and the internet in our daily life is the primary cause of the rise in financial theft and online scams [9, 10]. Cybercriminals are grabbing hold of possibilities to take advantage of weaknesses in digital platforms and human behavior as more individuals and businesses conduct transactions online. The swift growth of digital wallets, online banking, and e-commerce in India has created more opportunities for cyber fraud to thrive.

#### 1.1.1 Evolving Tactics of Cybercriminals

- **Phishing Attacks:** Among the most pervasive types of online scams, phishing attacks has evolved with many elaborated techniques like cloned websites and personalized messages designed to trick users that reveal sensitive information [10]. Closely related is identity theft, where cybercriminals exploit stolen personal data to gain unauthorized access to accounts, commit financial fraud, or impersonate victims. [11]. Such frauds are particularly effective because they exploit users' trust and lack of awareness. Often delivered through fake emails or messages, they lure individuals into disclosing private information such as credit card numbers or passwords. High-profile breaches involving major banks and social media platforms underscore the serious consequences of these attacks.

- **Cryptocurrency:** Online financial fraud has entered a new phase with the rise of cryptocurrency [12]. Despite the promise of secure and transparent transactions, blockchain technology has been misused for scams such as Ponzi schemes and crypto wallet hacks [13, 14]. The pseudonymous

nature of cryptocurrencies makes it difficult to trace transactions and recover stolen funds, further emboldening attackers. For example, the One Coin scam was one of the largest cryptocurrency frauds in history, duping investors out of nearly ₹33,000 crore (approximately $4 billion).

- **Social engineering attacks:** There has also been a significant rise in social engineering attacks, including romance scams and business email compromise (BEC). These schemes rely on psychological manipulation to trick victims into transferring money or revealing sensitive information. Advances in artificial intelligence [15] have even enabled fraudsters to create realistic deepfake audio and video clips, making these attacks even more difficult to detect.

### 1.2 Understanding and Mitigating the Impact

A study of the mechanisms, impacts, and mitigation strategies related to financial fraud and online scams is essential given their rising frequency. This article focuses on common types of scams, the technical and psychological factors that enable them, and the social consequences of these crimes.

#### 1.2.1 Impact and Mitigation

- **COVID-19:** Financial fraud and online scams became significantly more prevalent during the global COVID-19 pandemic [16]. Cybercriminals exploited vulnerabilities in unsecured networks and the surge in online activity as organizations and individuals transitioned to remote work. During this period, pandemic-related scams such as fraudulent stimulus checks, fake charity appeals, and counterfeit vaccine sales were widespread.
- **Financial Losses:** These frauds have a significant psychological and economic impact. Victims often suffer emotional distress, financial losses, and damaged credit. Companies may face operational disruptions, legal liabilities, and reputational harm. Moreover, the sheer volume and complexity of such crimes strain cybersecurity and law enforcement resources, underscoring the urgent need for preventive measures.
- **Recognizing and Avoiding Scams:** Tackling the surge in financial and online fraud requires a comprehensive, multi-pronged approach. Businesses must strengthen their cybersecurity infrastructure, while public awareness initiatives should empower individuals to recognize and avoid scams. To curb cross-border fraud, it is vital for governments and regulatory bodies to enact effective legislation and encourage international cooperation. Emerging technologies particularly AI-driven fraud detection systems can significantly enhance the early identification and prevention of such threats.

### 2. Increased Online Scams and Financial Frauds Methods

The growing reliance on online media and the increasing integration of the internet into daily life have contributed to the rise in financial fraud and online scams. As more individuals and businesses conduct transactions online, cybercriminals have seized the opportunity to exploit vulnerabilities in digital platforms and human behavior. The rapid expansion of digital wallets, internet banking, and e-commerce has further enabled fraud to thrive. The scope and complexity of these threats are evident in several high-profile bank frauds and online scams. Below are some of the most notable examples. [17-19]:

**Ponzi and Pyramid scams:** The primary distinction between the two types of fraud (Ponzi and Pyramid) is that Ponzi schemes typically only ask victims to invest money, with promised returns due at a later date. In contrast to Ponzi schemes, pyramid schemes typically give a victim the chance to "make" money by enlisting more individuals in the fraud. By ensuring bigger returns on investments with little risk, online

Ponzi scams have deceived millions of people. Digital communication can increase the spread of frauds like a notable case is the Saradha Chit Fund scam, which defrauded thousands of investors mostly in West Bengal and Odisha of nearly ₹2,500 crore. The company lured victims with promises of high returns through its chit fund schemes. The fallout included multiple arrests, political controversy, and widespread financial devastation among small investors. Similarly, in another case, two people were apprehended by the Indian police following the filing of a case against Falcon Invoice Discounting. The company had advertised returns of up to 22% and claimed to link investors with companies like Amazon (AMZN.O), Britannia (BRIT.NS) and others.

**Ransomware Attacks:** Attacks that restrict access to data or computer systems and demand a fee to unlock them have become increasingly common. Cybercriminals use ransomware to encrypt victims' data and demand payment usually in Bitcoin to restore access. Prominent incidents such as the WannaCry and REvil ransomware attacks have caused widespread damage by targeting governments, businesses, and hospitals. Examples include the 2017 WannaCry ransomware attack impacted several systems, including those of state-run enterprises like Gujarat State Wide Area Network (GSWAN), highlighting vulnerabilities in critical government infrastructure.

**Romance Scams:** In romance scams also known as catfishing or darling scams fraudsters create fake online identities to form emotional connections with victims, ultimately deceiving them into sending money or sharing personal information. Scammers often use fabricated stories about financial hardship, family emergencies, or travel expenses to solicit funds. These scams frequently begin on dating apps or social media platforms. By forming fictitious online relationships, romance scammers exploit emotional vulnerabilities to manipulate victims into transferring money. According to reports, such scams cost millions of dollars annually, with most victims being targeted through social media and dating sites. Examples include intimate activity scams, fake courier services, misleading personal stories, and more. In one case, a Delhi woman lost ₹50 lakh to a man posing as a UK doctor who promised gifts and then involved a fake customs officer demanding clearance fees. Similarly, a Pune woman was duped of ₹12 lakh by a man claiming to be an army officer seeking money for a fake emergency. In Mumbai, a woman lost ₹5 lakh to a Facebook friend pretending to be a UK engineer.

**Business Email Compromise (BEC):** In India, fraudsters use fake emails to trick employees within companies into transferring money or revealing confidential information. This tactic is known as Business Email Compromise (BEC). These attacks often rely on social engineering techniques to bypass security measures by impersonating trusted vendors or high-level executives. The objective of BEC schemes is to manipulate companies into making unauthorized payments by posing as executives or suppliers. In a major cyber fraud case in 2018, a group of fraudsters in India posed as top executives of an international company and used fake emails and forged documents to trick a Pune-based subsidiary of an Italian firm, Tecnimont Pvt. Ltd., into transferring ₹200 crore (approximately $27 million) to bank accounts in Hong Kong. The attackers used business email compromise (BEC) tactics mimicking senior executives and creating a sense of urgency to authorize the fund transfers over multiple transactions before the fraud was discovered.

**Tech Support Scams:** If someone claims there is an issue with your computer, end the call immediately. Even if the number appears genuine or local, an unexpected tech support call is likely a scam. These fraudsters often disguise

themselves as reputable or local businesses by manipulating caller ID information. Ignore any pop-ups urging you to contact tech support. Scammers impersonate legitimate tech support agents to deceive victims into paying for unnecessary services or granting remote access to their devices. The elderly are frequently targeted in these scams, as criminals exploit their limited familiarity with technology.

These well-documented incidents illustrate the adaptability and ingenuity of cybercriminals. The diverse strategies, objectives, and methods used in each case underscore the importance of staying vigilant and making continuous efforts to combat financial fraud and online scams. A Recent Changes page from a MediaWiki site affected by technical support scammers promoting fake "help lines"

### 2.1 Summary Table: Key Banking Fraud Statistics (2023–2025)

Banking fraud in India is rising rapidly, primarily driven by digital scams. While private banks report a higher number of cases, public sector banks incur greater financial losses. Internet and card-related frauds are the most prevalent, with mule accounts emerging as a hidden but serious threat. Authorities are intensifying enforcement efforts and increasing public reporting to address this growing concern.

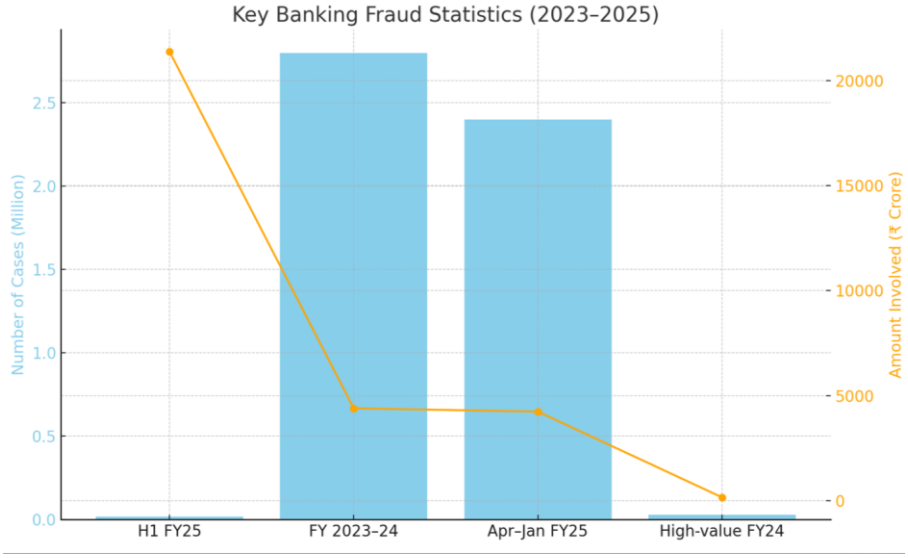


**Figure 2: Digital financial frauds [19]**

Banking frauds in India have seen a sharp rise in FY25, with losses exceeding ₹21,000 crore in just six months. Digital scams particularly those involving card fraud, social engineering, and mule accounts are the primary drivers of this surge. Despite regulatory actions and improved detection systems, the scale and sophistication of these frauds underscore the urgent need for stronger preventive measures and greater public awareness.

## 3. Key Remedies for Combating Online Scams and Financial Fraud:

A multifaceted strategy involving legislative frameworks, public education, and technological advancements is essential to combat financial fraud and online scams [20]. Table 1 provides a detailed explanation of several effective security techniques.

**Table 1: Anti-Fraud Measures**

| Strategy | Mechanism |
|---|---|
| Enhanced Authentication | Multi-factor authentication (MFA) enhances security by requiring users to verify their identity through multiple methods, such as passwords, biometrics, or one-time codes. Additionally, behavioral biometrics such as mouse movements and keystroke dynamics further strengthen security by detecting unusual user activity. |
| Intelligent Fraud Detection | Machine learning and artificial intelligence algorithms can quickly detect suspicious activity by analyzing patterns in online transactions. These systems support proactive responses to potential threats by using anomaly detection to identify deviations from normal user behavior. |
| Secure Data Protection | Sensitive information, including financial details and login credentials, is protected during transmission thanks to end-to-end encryption. The use of secure protocols like HTTPS and encrypted email services significantly reduces the risk of data interception by attackers. |
| User Vigilance & Training | Public awareness campaigns can educate people about common fraud schemes, warning signs, and safe online practices. Employers can help prevent human errors such as falling for phishing emails by regularly training staff in cybersecurity. |
| Policy & International Cooperation | Governments and regulatory agencies must enforce strict data protection regulations, while companies should be held accountable for implementing robust cybersecurity measures. Cross-border collaboration among law enforcement agencies can significantly enhance efforts to identify and apprehend cybercriminals operating globally. |
| Fraud-Protected Payment Systems | Payment gateways equipped with integrated fraud detection systems can identify and block unauthorized transactions. Tokenization is one such technique that minimizes the risk of data theft by replacing sensitive payment information with unique identifiers during transactions. |
| Blockchain-Enabled Security | Blockchain technology can improve financial transactions' security and transparency, making it harder for criminals to alter data. Contractual agreements can be automated and secured with smart contracts, lowering the possibility of tampering and human error. |
| Cyber Incident Management | To reduce harm during cyberattacks, organizations should set up explicit incident response procedures, such as identifying and alerting stakeholders and isolating compromised systems. In the event of ransomware attacks or other security breaches, regular backups of important data can guarantee quick recovery. |
| Joint Cybersecurity Ventures | Governments, businesses, and nonprofit organizations working together can increase the scope and efficacy of anti-fraud campaigns. Cooperation might concentrate on standardizing cybersecurity procedures, enhancing reporting systems, and providing funds for the development of novel solutions. |

Integrating these solutions can strengthen the digital ecosystem's resistance against financial fraud and online scams, preventing serious harm to both people and businesses.

## 4. Challenges with Current Solutions:

The development of comprehensive security solutions has lagged behind the rise of financial crime and internet scams, creating a difficult situation for governments, businesses, and individuals [22]. A detailed examination of the difficulties with the security solutions available today is provided in Table 2.

**Table 2: Challenges with current solutions**

| Challenge | Description |
|---|---|
| Response Latency | The inability of many current systems in order to get data responsive in real time means that fraudulent transactions might not be discovered until the money has been abducted. Sharp attackers' number of times overcome the real time verification process. |
| Limited Resources | Smaller businesses frequently don't have the funds to put strong security measures in place. Also, effective threat monitoring, analysis, and response are hampered by a lack of cybersecurity experts. |
| Next-Gen Cyber Risks | The widespread adoption of Internet of Things (IoT) devices presents a major security challenge, as many are developed without robust security features. This inherent vulnerability makes them prime targets for cybercriminals seeking to infiltrate networks and carry out malicious activities. |
| Internal Security Risks | Malicious insiders or inadequately trained personnel can often bypass security protocols. Among all types of fraud, insider threats are particularly difficult to detect and mitigate. |
| Dynamic Threat Environment | The continual evolution of fraudulent techniques in response to advanced security protocols reflects an ongoing "arms race" within the cybersecurity domain. This dynamic threat landscape inherently challenges the long-term effectiveness of static defense systems. |

The constant evolution of cybercriminal tactics, coupled with the rapid expansion of the digital landscape, poses a complex and dynamic challenge to financial security. Existing safeguards are struggling to keep pace with increasingly sophisticated threats and the growing attack surface. Until security measures strike a balance between robust protection and user convenience and global standards are firmly established consumers and businesses will remain vulnerable to financial fraud.

## 5. Conclusion:

In conclusion, the rise in sophisticated online scams and financial fraud highlights the urgent need for smarter, more adaptive security solutions. Traditional defenses are no longer adequate, as cybercriminals increasingly exploit technologies such as AI, blockchain, and social engineering [21]. This review summarizes the key types of online scams and financial frauds prevalent in the digital age. The ongoing battle between attackers and defenders reveals critical gaps in real-time detection, cross-platform coordination, and user education. Additionally, the widespread use of IoT devices and the rise of social engineering tactics further underscore the need for a unified, comprehensive approach to cybersecurity. Future efforts must prioritize proactive strategies that leverage real-time analytics and privacy-focused technologies to stay ahead of emerging threats. Developing fraud prevention techniques capable of identifying and mitigating risks before they

materialize should be a key focus of future research. This includes harnessing machine learning, real-time analytics, and privacy-preserving tools. Establishing adaptive security frameworks and global standards will require collaborative efforts between public and private sectors. Cybersecurity must evolve in parallel with the continuous expansion of the digital ecosystem. Sustained cooperation, innovation, and a forward-looking approach will be critical to ensuring a secure, resilient, and trustworthy digital financial environment.

**References**

[1] Gill, S. S., Wu, H., Patros, P., Ottaviani, C., Arora, P., Pujol, V. C., ... & Buyya, R. (2024). Modern computing: Vision and challenges. Telematics and Informatics Reports, 13, 100116.

[2] Sergeyev, A. Y., & Shirokova, O. V. (2023). Fraud in a digital society in the context of social change. Цифровая социология/Digital Sociology, 60.

[3] Yanamala, A. K. Y. (2024). Emerging challenges in cloud computing security: A comprehensive review. International Journal of Advanced Engineering Technologies and Innovations, 1(4), 448-479.

[4] Nosál, J. (2023). Crime in the digital age: A new frontier. In The Implications of Emerging Technologies in the Euro-Atlantic Space: Views from the Younger Generation Leaders Network (pp. 177-193). Cham: Springer International Publishing.

[5] Ahmed, M., Ansar, K., Muckley, C. B., Khan, A., Anjum, A., & Talha, M. (2021). A semantic rule based digital fraud detection. PeerJ Computer Science, 7, e649.

[6] BENSAID, A., & DRAOUI, H. (2024). Proving Cyber-Crime Using Modern Technology: Artificial Intelligence as A Model (Doctoral dissertation, ibn khaldoun university-Tiaret).

[7] Agarwal, U., Rishiwal, V., Tanwar, S., & Yadav, M. (2024). Blockchain and crypto forensics: Investigating crypto frauds. International Journal of Network Management, 34(2), e2255.

[8] Latha, S. B., Dastagiraiah, C., Kiran, A., Asif, S., Elangovan, D., & Reddy, P. C. S. (2023, August). An Adaptive Machine Learning model for Walmart sales prediction. In 2023 International Conference on Circuit Power and Computing Technologies (ICCPCT) (pp. 988-992). IEEE.

[9] Modise, J. M. (2023). Community Policing Strategies Include Community Patrols, Neighborhood Watch and Community Policing. International Journal of Innovative Science and Research Technology, 8(7), 3458-3476.

[10] Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. Blockchain: research and applications, 3(2), 100067.

[11] Patel, B., Vasa, J., & Mewada, H. (2024). e-Prime-Advances in Electrical Engineering, Electronics and Energy.

[12] Saha, S., Hasan, A. R., Mahmud, A., Ahmed, N., Parvin, N., & Karmakar, H. (2024). Cryptocurrency and financial crimes: A bibliometric analysis and future research agenda. Multidisciplinary Reviews, 7(8), 2024168-2024168.

[13] Roosenboom, P., van der Kolk, T., & de Jong, A. (2020). What determines success in initial coin offerings?. Venture Capital, 22(2), 161-183.

[14] Chiu, T., Chiu, V., Wang, T., & Wang, Y. (2022). Using textual analysis to detect initial coin offering frauds. Journal of Forensic Accounting Research, 7(1), 165-183.

[15] Maji, S. K., & Laha, A. (2023). Role of financial and digital literacy in determining digital transaction behaviour: evidence from student level survey in West Bengal (India). International Journal of Business

Environment, 14(2), 183-210.

[16] Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & security, 105, 102248.

[17] Thakur, K., Ali, M. L., Obaidat, M. A., & Kamruzzaman, A. (2023). A systematic review on deep-learning-based phishing email detection. Electronics, 12(21), 4545.

[18] Patel, K. (2023). Credit card analytics: a review of fraud detection and risk assessment techniques. International Journal of Computer Trends and Technology, 71(10), 69-79.

[19] https://economictimes.com/industry/banking/finance/banking/banking-frauds-rise-in-h1fy25-amount-involved-jumps-8-time-rbi-report/articleshow/116685504.cms

[20] Luo, J., Luo, J., Nan, G., & Li, D. (2023). Fake review detection system for online E-commerce platforms: A supervised general mixed probability approach. Decision Support Systems, 175, 114045.

[21] Bachmann, N., Tripathi, S., Brunner, M., & Jodlbauer, H. (2022). The contribution of data-driven technologies in achieving the sustainable development goals. Sustainability, 14(5), 2497.