Available in online @ www.iaraindia.com
RESEARCH EXPLORER-International Journal on Economic and Business Management
ISSN: 2250-1940 (P) 2349-1647 (O)
Impact Factor: 3.655(CIF), 2.78(IRJIF), 2.77(NAAS)
Volume XIV, Issue 48 (2)
July - September 2025
Formally UGC Approved Journal (63185), © Author

DETAILED INSIGHTS INTO EMERGING CYBER THREATS AND CURRENT SECURITY DYNAMICS

Dr. MOHANA PRIYA .M
Assistant Professor and Research Supervisor
Department of Commerce
Vels Institute of Science, Technology and Advanced Studies
Pallavaram, Chennai

Dr. VANITHA P
Assistant Professor and Research Supervisor
Department of Commerce
Vels Institute of Science, Technology and Advanced Studies,
Pallavaram, Chennai

ABSTRACT

In today's digital era, cyber fraud poses a significant threat to individuals, organizations, and governments alike. This research examines newspaper articles to explore various types of cybercrimes, financial losses, and threats to online safety. It sheds light on prevalent scams such as bogus investment opportunities, phishing schemes, ransomware attacks, AI-driven cybercrimes, and frauds carried out through social media. By analysing the profiles of the victims, the study identifies the most affected groups and quantifies the monetary losses, which range from thousands to crores of rupees. The study underscores the urgent need to enhance cybersecurity measures, raise public awareness, and implement stricter regulations to combat these escalating threats.

KEYWORDS: Cyberfraud, AI-based cybercrime, investment fraud, social media scams, cyber security risks, financial losses, cyber threats.

INTRODUCTION

In the modern digital age, cyber fraud is emerging as a serious concern for individuals, businesses, and government bodies. Daily newspaper reports reveal how cybercriminals take advantage of vulnerabilities in digital systems. Analysing these reports provides valuable insights into current cyber threats, the extent of financial damage, and strategies for prevention. This research paper analyses newspaper coverage of cyber fraud, classifying various forms of cybercrime and evaluating their wider implications. Major Cyber Threats

1. **DigitalArrestScams**
   - Fraudsters impersonate law enforcement and trick victims into paying large sums to avoid fake legal trouble.
   - Seniorcitizensaretheprimarytargets.
2. **FakeInvestmentScams**
   - Cybercriminal sure victims with promises of high returns in stock trading, cryptocurrency, and investment platforms.
   - Victims invest large amounts but never receive their returns.

3. **AI-BasedCybercrime**
   - Fraudsters use AI-generated voices and deep fake technology to manipulate victims.
   - AI-powered phishing attacks are becoming more sophisticated.
4. **Work-From-Home Frauds**
   - Victims, including students and homemakers, are tricked into paying for fake job opportunities.
   - Millions of rupees have been lost in such scams.
5. **Social Media Frauds**
   - Scammers use WhatsApp and Facebook to gain victims' trust and extort money.
   - Fake friendship requests and WhatsApp KYC scams are rising.
6. **Bank and Financial Frauds**
   - Victims are tricked into sharing OTPs and passwords.
   - Fraudsters use phishing links to steal bank details.
7. **Bluetooth and Phone Hacking**
   - HackersexploitBluetoothvulnerabilitiestoaccessdeviceswithoutconsent.
   - Malicious mobile apps steal personal data.

Emerging Cyber Trends

- **Government Crackdown on Cybercrime**: More scammers are being arrested, and cyber security awareness campaigns are increasing.
- **Growth of Cyber Insurance**: More people are purchasing cyber insurance to protect against fraud losses.
- **AI in cyber security**: AI is being used not only by criminals but also by security agencies to detect and prevent cyber fraud.
- **Stricter Cyber security Laws**: Governments are introducing new laws to combat financial fraud and cyber threats.
- **Increase in Cybercrime Reporting**: More victims are reporting cyber fraud instead of staying silent.

How to Stay Safe

- Do not disclose OTPs, passwords, or any financial information during phone conversations.
- Refrain from opening unfamiliar links received through WhatsApp, email, or text messages.
- Stay alert and sceptical of investment offers that guarantee fast or high returns.
- Confirm the authenticity of unknown callers who say they are from law enforcement.
- Activate two-factor authentication (2FA) to enhance your account’s security.
- Regularly update software and mobile apps to protect against hacking attempts.

LITRATURE REVIEW

Research shows that cyber fraud has progressed past conventional phishing attacks, now incorporating advanced methods like deepfake technology, artificial intelligence-driven scams, and ransomware incidents (Smith & Johnson, 2022).The growing dependence on mobile apps for handling financial transactions has contributed to a surge in fake investment schemes and deceptive trading applications (Patel, 2023). Furthermore, recent years have seen a rise in social engineering methods such as impersonation fraud and digital arrest scams (Kumar & Singh, 2021).

CYBERSECURITYMEASURESANDRISKMITIGATION

To tackle cyber fraud, experts highlight the importance of raising public awareness, enhancing financial oversight, and enforcing stricter cybersecurity regulations (Rao & Desai, 2024). Recommended preventive strategies include the use of two-factor authentication (2FA), secure digital banking platforms, and AI-powered fraud detection tools (Williams, 2023). Moreover, government-led efforts such as introducing cyber insurance schemes and setting up dedicated

fraud helplines aim to offer victims legal and financial assistance (Mehta, 2024).

An analysis of news coverage from publications like Lokmat, Loksatta, Sakal, The Times of India, The Indian Express, and Maharashtra Times between July 2024 and January 2025 indicates a notable rise in cyber fraud cases across India. This increase is largely linked to the widespread adoption of digital payment systems and the increasingly sophisticated methods used by cybercriminals.

OBJECTIVES

Themain objectives of this studyare:

1. **Identify Key Entities:** Examine and categorize the people involved, financial information, and digital platforms referenced in incidents of cyber fraud.
2. **Examine Financial Transactions:** Evaluate financial amounts, measured in lakhs and crores, to detect patterns or identify any irregularities.
3. **Profile Victims and Criminals:** Analyze the demographic profiles of both victims and fraudsters, focusing on their age, occupations, and economic status.
4. **Analyse Digital and Financial Risks:** Examine the cybersecurity threats linked to digital fraud, financial transactions, and investment platforms.
5. **DetectAnomalies:** Detect anomalies by pinpointing irregular transactions, unusual patterns, and emerging risks.
6. **Understand the Role of Applications:** Examine the use of apps in financial transactions and their involvement in fraud cases.

ANALYTICAL FRAMEWORK

Monthly Distribution of Cybercrime Incidents

Cyber-related news was most prominent in July 2024, indicating a high level of activity during that period. August 2024 also saw numerous reports, showing that cyber issues remained a key focus. Another notable increase occurred in January 2025. In contrast, June and December 2024 had minimal coverage, suggesting limited cyber activity during those months. Overall, the highest volume of cyber news appeared in mid to late 2024, with a renewed surge at the beginning of 2025.

Methods Used by Cybercriminals

- Fraudulent Apps and APKs: Cybercriminals deploy fake applications like the "CMS Trading App" and "Zeroda investment scam" to gather sensitive personal information.
- Investment and Stock Market Fraud: Terms such as "forex trading fraud," "block trading scam," and "parcel scam" indicate that scammers exploit investment platforms for financial gain.
- Phishing and Deceptive Websites: Victims are misled by bogus KYC update prompts, fake bank notifications, and scams like the "Post Office" or "FedEx courier" hoaxes, which aim to capture confidential details.
- Ransomware and Coercive Tactics: References to "ransomware attacks," "digital arrest incidents," and fraudulent "CBI investigations" suggest that intimidation is used to extort money from individuals.

Demographic Analysis

Cyber fraud victims come from various age groups and occupational backgrounds, showing that cybercriminals target a broad spectrum of individuals.

Age Group Analysis

- Victims span a wide age range, from individuals in their 30s to senior citizens in their late 70s.
- Most cases involve people aged between 40 and 70.
- Prominent examples include a 73-year-old male victim, a 64-year-old former army officer, and a 74-year-old elderly individual.
- Middle-aged professionals, including those aged 45 and 48, have also been among the targets.

Occupational Analysis:

- Victims include professionals like doctors, engineers, IT specialists, and entrepreneurs.
- A retired banking official and an airline employee have also fallen prey to cyber fraud.
- Several cases involve individuals working in private sector companies.
- Women, including homemakers and widows, are also among those targeted by cybercriminals.

KEY FINDINGS:

- Surge in Large-Scale Cyber Frauds: According to the Indian Ministry of Finance, incidents of cyber fraud involving sums over ₹1 lakh rose more than four times in the fiscal year ending March 2024, with total losses exceeding ₹177 crore.
- Overall, Losses from Digital Payment Scams: Data from the Reserve Bank of India revealed that digital payment frauds led to a total loss of nearly ₹1,450 crore during the same timeframe.
- Sophisticated Fraud Methods: Cybercriminals used advanced tactics such as impersonating authorities and leveraging AI-generated deepfakes to trick victims into sharing personal data or transferring money.

Government and Regulatory Responses:

Telecom Regulatory Authority of India(TRAI): Steps have been taken to block spam callers and reduce fraudulent communications.

Reserve Bank of India (RBI): Suggested regulations permitting banks to temporarily freeze accounts suspected of involvement in fraudulent activities.

Public Awareness Campaigns: The government introduced campaigns involving celebrities to raise public awareness about identifying and preventing cyber fraud.

Preventative Measures for Individuals:

Verify Communications: Always verify the authenticity of individuals or organizations before sharing personal details or carrying out financial transactions.

Stay Informed: Regularly update yourself on common cyberfraud tactics and remain vigilant against suspicious activities.

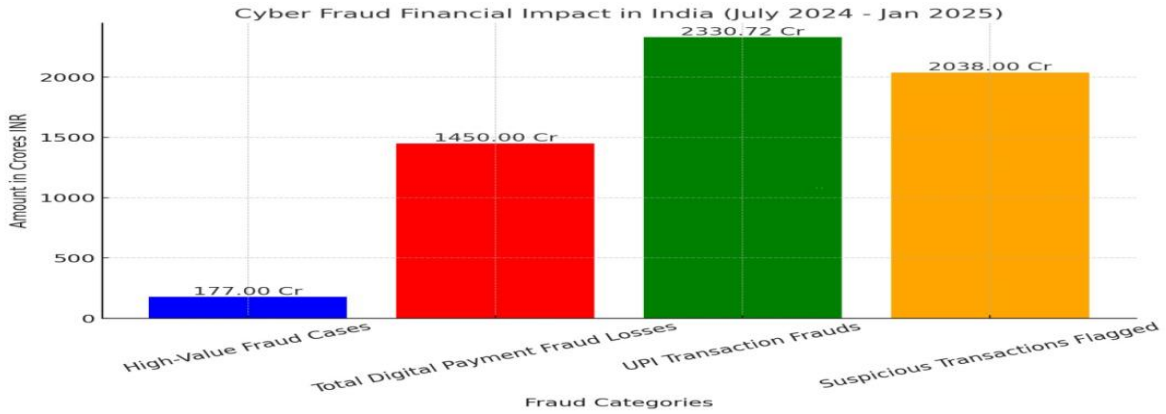
Secure Personal Information:

Use strong, unique passwords for online accounts and enable two- factor authentication where possible.

Thisanalysisunderscoresthecriticalneedforheightenedcybersecurityawarenessandproactive measures to protect against the growing threat of cyber fraud in India's digital landscape. Analyzing data from Government of India publications reveals a significant increase in cyberfraud incidents and associated financial losses between July 2024 and January 2025

Financial Impact of Cyber Frauds

Total Fraud Amount: In the fiscal year 2024-25 (up to January 2025), the total amount involved in frauds reached ₹18,120.82 crore, with ₹2,330.72 crore attributed to Unified Payments Interface (UPI) transaction frauds.



Government Initiatives to Tackle Cyber Fraud:

- Deactivation of Fraudulent SIM Cards and IMEIs: By February 28, 2025, the Government of India, acting on inputs from law enforcement agencies, had deactivated over 7.81 lakh SIM cards and blocked 2,08,469 IMEIs in an effort to suppress fraudulent communications. (Source: Press Information Bureau)
- Detection of Mule Accounts: Authorities have uncovered more than 19 lakh mule bank accounts, with suspicious transactions amounting to ₹2,038 crore flagged—demonstrating proactive financial fraud detection.
- Citizen-Focused Reporting Mechanism: The Ministry of Home Affairs introduced the National Cyber Crime Reporting Portal (https://cybercrime.gov.in), enabling individuals to report a wide range of cybercrimes and aiding in more effective tracking and enforcement. (Source: Press Information Bureau)

These initiatives underscore the government's dedication to reducing cybercrime and enhancing digital financial security for Indian citizens.

Note: This summary is based on data available as of March 27, 2025. For the latest updates, consult official government releases and financial authority reports.

CONCLUSION

Cyber threats are advancing swiftly, with cybercriminals leveraging sophisticated technologies to target both individuals and organizations. This analysis emphasizes the urgent need for enhanced cybersecurity frameworks, increased public awareness, and more stringent legal action against offenders. Staying informed and implementing cybersecurity best practices are essential steps to minimize financial losses and protect sensitive personal information from malicious intrusions.

REFERENCES

1. Gupta, A., Sharma, R., & Mehta, P. (2024). Cybercrime and Financial Fraud: A Socio-Economic Analysis. Cyber Security Journal, 12(3), 56-72.
2. Kumar, S., & Singh, P. (2021). Social Engineering Attacks and Their Impact on Digital BankingUsers. International Journal of Cyber Studies, 9(2), 112-130.
3. Mehta, K. (2024). The Role of Government Policies in Combating Cyber Fraud. Journal of Digital Security, 15(1), 23-40.
4. Patel,V.(2023).InvestmentFraudandFakeTradingApps:AnEmergingThreat.FinancialCybersecurity Review, 10(4), 88-105.
5. Rao, L., & Desai, N. (2024). CybersecurityRegulations and Their Effectiveness Against Financial Crimes. International Cyber Law Journal, 14(2), 134-150.
6. Sharma,M.,&Verma,K.(2023).CryptocurrencyFraudsandStockMarketManipulationsin India. Economic Crimes Journal, 8(1), 47-65.
7. Smith,J.,&Johnson,D.(2022).TheEvolutionofCyberFraud:FromPhishingtoAI-based Attacks. Journal of Cybercrime Research, 11(2), 98-120.
8. Williams,T.(2023).AIinCybersecurity:ADouble-

EdgedSword.ArtificialIntelligenceand
9. Cyber Defense, 9(3), 67-89.