IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CYBER SECURITY THREATS AND TRENDS : AN ANALYTICAL STUDY

Mrs.Rajratan Sachin Gavhane
Librarian, B.D.Karve College of Arts, Commerce and Science

Abstract
In today's digital world, cyber fraud is a big threat to people, businesses, and governments. This study looks at newspaper reports on cyber fraud to understand different types of crimes, the money lost, and the risks to online security. It highlights common scams like fake investment schemes, phishing attacks, ransom ware, AI-based cybercrime, and social media fraud. By studying the victims, the research shows who is most affected and how much money is lost, ranging from thousands to crores of rupees. The findings stress the need for better cyber security, more public awareness, and stricter laws to fight these growing threats.

Keywords
Cyber fraud, financial scams, phishing, ransom ware , AI-based cybercrime, investment fraud, social media scams, cyber security risks, financial losses, cyber threats.

Introduction
In today's digital world, cyber fraud is becoming a major problem for individuals, businesses, and even government institutions. Every day, newspapers report cases of cybercrime, showing how fraudsters exploit weaknesses in digital systems. Studying these reports helps us understand the latest threats, financial losses, and ways to prevent such crimes. This research paper focuses on newspaper reports related to cyber fraud, categorizing different types of crimes and assessing their broader impact.

Major Cyber Threats

1. **Digital Arrest Scams**
   - Fraudsters impersonate law enforcement and trick victims into paying large sums to avoid fake legal trouble.
   - Senior citizens are the primary targets.
2. **Fake Investment Scams**
   - Cybercriminals lure victims with promises of high returns in stock trading, crypto currency, and investment platforms.
   - Victims invest large amounts but never receive their returns.
3. **AI-Based Cybercrime**
   - 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**
    - Hackers exploit Bluetooth vulnerabilities to access devices without consent.
    - 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

- Never share OTPs, passwords, or financial details over the phone.
- Avoid clicking on unknown links in WhatsApp, emails, or SMS.
- Be cautious of investment schemes promising quick profits.
- Verify the identity of unknown callers claiming to be law enforcement officers.
- Enable two-factor authentication (2FA) for added security.
- Keep software and mobile apps updated to prevent hacking.

Literature Review

Cyber security threats have evolved significantly, with financial fraud being a major concern for individuals, businesses, and governments. Researchers have examined various aspects of cyber fraud, including the methods employed by cybercriminals, the demographics of victims, and the financial impact of these crimes.

Cyber Fraud Trends and Techniques

Studies indicate that cyber fraud has expanded beyond traditional phishing scams to include sophisticated techniques such as deepfake technology, AI-generated fraud, and ransomware attacks (Smith & Johnson, 2022). The increasing reliance on mobile applications for financial transactions has also led to the rise of fraudulent investment platforms and fake trading apps (Patel, 2023). Additionally, social engineering tactics, including impersonation scams and digital arrest fraud, have been frequently reported in recent years (Kumar & Singh, 2021).

Victim Demographics and Financial Impact

Research suggests that cybercriminals target a broad spectrum of individuals, ranging from young professionals to senior citizens. While younger victims are often lured into work-from-home scams and investment frauds, older individuals are frequently targeted through digital arrest scams and phishing attacks (Gupta et al., 2024). Financial losses vary widely, with reports indicating that individuals have lost amounts ranging from a few thousand rupees to several crores. Large-scale frauds involving crypto currency and stock market scams have also been on the rise (Sharma & Verma, 2023).

Cybersecurity Measures and Risk Mitigation

To combat cyber fraud, researchers emphasize the need for public awareness, financial monitoring, and stricter cyber security laws (Rao & Desai, 2024). The implementation of two-factor authentication (2FA), secure financial applications, and AI-based fraud detection systems has been suggested as an effective preventive measure (Williams, 2023). Additionally, government initiatives, such as cyber insurance policies and financial fraud hotlines, have been proposed to provide victims with legal and financial support (Mehta, 2024).

Analysing reports from newspapers such as Lokmat, Loksatta, Sakal, The Times of India, The Indian Express and Maharashtra Times between July 2024 and January 2025 reveals a significant increase in cyber fraud incidents across India. This surge is attributed to the rapid adoption of digital payments and the evolving tactics of cybercriminals.

Objectives

The main objectives of this study are:

1. **Identify Key Entities** – Analyse and classify individuals, financial details, and digital applications mentioned in cyber fraud cases.
2. **Examine Financial Transactions** – Assess monetary values (in lakhs and crores) to identify trends or unusual patterns.
3. **Profile Victims and Criminals** – Understand the demographics of victims and fraudsters, including their age, profession, and financial background.
4. **Analyse Digital and Financial Risks** – Investigate cyber security risks associated with digital fraud, financial markets, and investment schemes.
5. **Detect Anomalies** – Identify irregular transactions, suspicious patterns, and emerging threats.
6. **Understand the Role of Applications** – Examine the use of apps in financial transactions and their involvement in fraud cases.

Analytical Framework

1. **Monthly Distribution of Cybercrime Incidents**

- The most cyber news came in **July 2024**, meaning a lot happened in that month. **August 2024** also had many news reports, so cyber topics stayed important. Then, in **January 2025**, there was another rise in news.
- On the other hand, **June 2024** and **December 2024** had very few cyber news articles, meaning not much happened then.
- Overall, cyber news was most active in the middle and end of 2024, with another spike at the start of 2025.

2. **Methods Used by Cybercriminals:-**

- Fake Apps & APKs: **Cybercriminals use fraudulent apps, like "CMS Trading App" and "Zeroda investment scam," to steal personal data.**
- **Fake Investment & Stock Market Scams:** Keywords such as "forex trading fraud," "block trading scam," and "parcel scam" suggest that fraudsters manipulate investment platforms.
- **Phishing & Fake Websites:** Fraudulent KYC updates, fake bank notices, and "Post Office and FedEx courier scams" trick victims into revealing credentials.
- **Ransomware & Digital Arrests:** The mention of "ransomware attack," "digital arrest cases," and "CBI investigation fraud" implies the use of scare tactics to extort money.

3. **Demographic Analysis**

- The victims of cyber fraud belong to diverse age groups and professions, indicating that cybercriminals target a wide range.

4. **Age Group Analysis:**

- The victims range from young adults (30 years old) to senior citizens (78 years old).
- The majority of victims fall within the 40–70 age range.
- Notable cases include a **73-year-old man**, a **64-year-old army veteran**, and a **74-year-old senior citizen**.
- Several middle-aged individuals, such as **45-year-old and 48-year-old professionals**, have also been targeted.

5. **Occupational Analysis:**

- Affected individuals include professionals such as **doctors, engineers, software engineers, and businesspersons**.
- A **retired bank manager and an airline staffer** are also among the victims.
- Some victims are **employees of private firms**.
- Women, including **widows and homemakers**, are also among those affected.

Key Findings:- Digital Payment Fraud in India: Trends, Financial Impact, and Policy Interventions

- **Rise in High-Value Cyber Fraud Cases:** The Indian Ministry of Finance reported that high-value cyber fraud cases (involving amounts exceeding ₹1 lakh) increased more than fourfold in the fiscal year ending March 2024, resulting in losses exceeding ₹177 crore.
- **Total Digital Payment Fraud Losses:** The Reserve Bank of India noted that total digital payment fraud amounted to approximately ₹1,450 crore during the same period.
- **Common Fraud Techniques:** Scammers employed advanced methods, including impersonating officials and utilizing artificial intelligence to create deep fake content, deceiving individuals into transferring funds or divulging sensitive information.

Government and Regulatory Responses:

- **Telecom Regulatory Authority of India (TRAI):** Implemented measures to blacklist spam callers and curb fraudulent communications.
- **Reserve Bank of India (RBI):** Proposed guidelines allowing banks to freeze accounts suspected of being used for fraudulent activities. Mary J. Moyer Blog - Hana Quinn+6Reuters+6Reuters+6
- **Public Awareness Campaigns:** The government launched initiatives featuring celebrities to educate citizens on recognizing and avoiding cyber fraud.

Preventative Measures for Individuals:

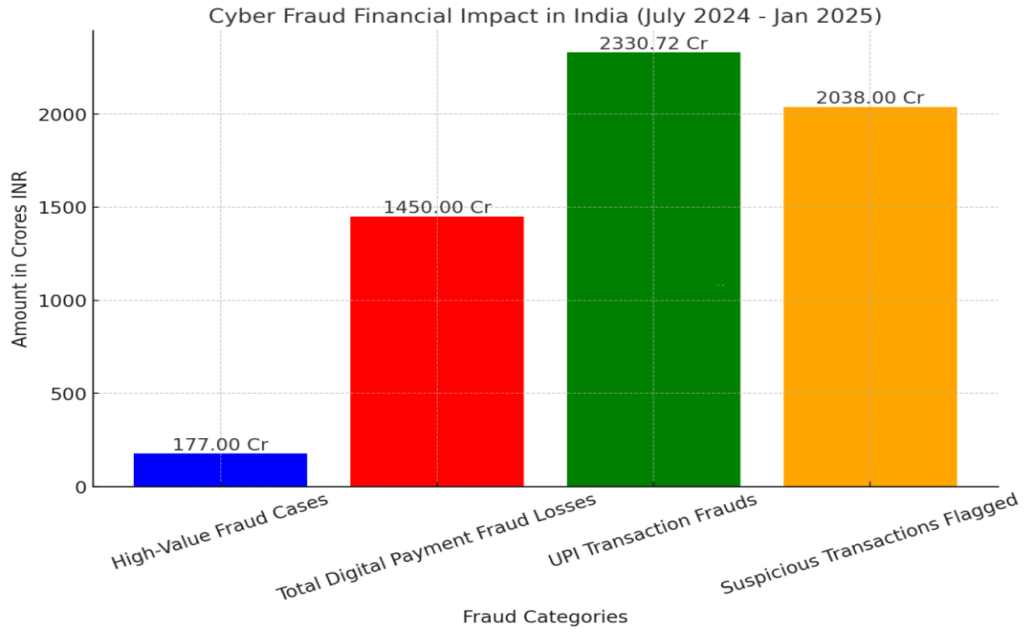
- **Verify Communications:** Always confirm the identity of individuals or organizations before responding to requests for personal information or financial transactions.
- **Stay Informed:** Regularly update yourself on common cyber fraud tactics and remain vigilant against suspicious activities.
- **Secure Personal Information:** Use strong, unique passwords for online accounts and enable two-factor authentication where possible.

This analysis underscores the critical need for heightened cyber security awareness and proactive measures to protect against the growing threat of cyber fraud in India's digital landscape.

Analysing data from Government of India publications reveals a significant increase in cyber fraud 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 Measures to Combat Cyber Fraud:

- **Blocking Unauthorized SIM Cards and IMEIs:** As of February 28, 2025, the Government of India, based on reports from police authorities, has blocked over 7.81 lakh SIM cards and 2,08,469 IMEIs to curb fraudulent activities. Press Information Bureau
- **Identifying Mule Accounts:** More than 19 lakh mule accounts have been identified, and suspicious transactions worth ₹2,038 crore have been flagged, indicating proactive measures to detect and prevent fraudulent financial activities.
- **Public Reporting Initiatives:** The Ministry of Home Affairs has launched the National Cyber Crime Reporting Portal (https://cybercrime.gov.in) to enable the public to report all types of cybercrimes, facilitating better tracking and action against cyber fraud. Press Information Bureau

These efforts reflect the government's commitment to mitigating cyber fraud and protecting citizens from digital financial crimes.

Note: The above analysis is based on data available up to March 27, 2025. For the most current statistics and information, please refer to official government publications and financial institution reports.

Conclusion

Cyber threats are evolving rapidly, with criminals using advanced technology to exploit individuals and businesses. This study highlights the need for stronger cyber security measures, public awareness, and stricter legal actions against cybercriminals. By staying informed and adopting cyber security best practices, we can reduce financial losses and safeguard personal data from malicious attacks.

Scope and Limitations

Scope

- **Financial Analysis**: Study financial transactions, identify anomalies, and analyse cyber fraud patterns.
- **Victim and Criminal Profiling**: Categorize individuals based on age, gender, and profession to understand their roles in cyber fraud cases.
- **Digital and Financial Applications**: Evaluate the involvement of various apps in financial fraud and cyber security threats.
- **Correlation between Digital and Financial Activities**: Understand the links between online transactions and financial scams.

Limitations

- **Incomplete Data**: Some financial details may be missing or incomplete, affecting accuracy.
- **Lack of Real-Time Data**: Findings are based on past reports and may not reflect on-going cybercrime activities.
- **Legal and Regulatory Constraints**: The study does not have access to official financial records, limiting its ability to confirm fraud cases legally.

Recommendations

- **Increase Public Awareness**: Educate people, especially senior citizens, about cyber security risks.
- **Strengthen Cyber security Measures**: Encourage the use of two-factor authentication and secure financial transactions.
- **Stronger Legal Actions**: Authorities must enforce stricter regulations to track and prosecute cybercriminals.
- **Financial Monitoring**: Banks and financial institutions should implement better fraud detection systems.

By implementing these measures, we can create a safer digital environment and protect individuals from cyber fraud.

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 Banking Users. 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). Investment Fraud and Fake Trading Apps: An Emerging Threat. Financial Cybersecurity Review, 10(4), 88-105.
5. Rao, L., & Desai, N. (2024). Cybersecurity Regulations and Their Effectiveness Against Financial Crimes. International Cyber Law Journal, 14(2), 134-150.
6. Sharma, M., & Verma, K. (2023). Cryptocurrency Frauds and Stock Market Manipulations in India. Economic Crimes Journal, 8(1), 47-65.
7. Smith, J., & Johnson, D. (2022). The Evolution of Cyber Fraud: From Phishing to AI-based Attacks. Journal of Cybercrime Research, 11(2), 98-120.
8. Williams, T. (2023). AI in Cybersecurity: A Double-Edged Sword. Artificial Intelligence and Cyber Defense, 9(3), 67-89.
9. **"लोकमत"** is the most frequently mentioned newspaper, appearing **89 times**. This suggests it is a major source for cyber news in the list.
10. **"सकाळ"** comes next with **15 mentions**, showing it also plays a role but much less than "लोकमत."
11. **"लोकसत्ता"** appears **6 times**, meaning it contributes some news but not as much.
12. **"पुढारी"** is mentioned just **once**, so it is a minor source.
13. **Press Information Bureau.** (2025, March 12). Steps taken to address the issue of digital arrest scams. Government of India. Retrieved from https://pib.gov.in
14. **Press Information Bureau.** (2025, March 18). Steps to curb cyber crime. Government of India. Retrieved from https://pib.gov.in
15. **Press Information Bureau.** (2025, February 11). Government actions on suspicious transactions and mule accounts. Government of India. Retrieved from https://pib.gov.in
16. **Press Information Bureau.** (2025, March 11). Preventive steps against UPI frauds. Government of India. Retrieved from https://pib.gov.in
17. **Press Information Bureau.** (2025, February 28). SIM cards and IMEIs blocked in response to cybercrime. Government of India. Retrieved from https://pib.gov.in
18. **Indian Cybercrime Coordination Centre (I4C).** (2024, February 26). Cyber Digest. Ministry of Home Affairs. Retrieved from https://cybercrime.gov.in
19. **Indian Cybercrime Coordination Centre (I4C).** (2024, February 7). Cyber Digest. Ministry of Home Affairs. Retrieved from https://cybercrime.gov.in
20. **Indian Cybercrime Coordination Centre (I4C).** (2025, March 25). Daily Digest. Retrieved from https://cybercrime.gov.in
21. **The Indian Express.** (2024, August 25). 272 Pune residents lost a staggering Rs 125 crore to share trading frauds. Retrieved from https://indianexpress.com
22. **The Indian Express.** (2024, August 22). Investment trainer in Pune duped of Rs 35 lakh in share trading fraud. Retrieved from https://indianexpress.com
23. **The Indian Express.** (2025, January 1). Bombay HC lawyer defrauded of Rs 1.58 crore in share trading scam. Retrieved from https://indianexpress.com
24. **The Indian Express.** (2025, January 28). Threatened with 'digital arrest', Pune senior citizen loses Rs 4.37 crore. Retrieved from https://indianexpress.com
25. **The Indian Express.** (2025, January 3). Cyber threats in 2024: Key incidents and expectations for 2025. Retrieved from https://indianexpress.com
26. **The Indian Express.** (2025, April 7). Pune police issue advisory on whale phishing attacks. Retrieved from https://indianexpress.com
27. **The Times of India.** (2024, August 6). In Mumbai, cyber cops recover Rs 100 crore due to timely helpline. Retrieved from https://timesofindia.indiatimes.com
28. **The Times of India.** (2025, January 22). Banker held for Rs 72 lakh con linked to cyber fraud. Retrieved from https://timesofindia.indiatimes.com
29. **The Indian Express.** (2024, July 19). Online job and fake loan frauds cost nearly Rs 600 crore in 2024. Retrieved from https://indianexpress.com