International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Cyber Frauds in India - An Investigation of Technological & Psychological Perspectives

Srihari Subudhi[1], Dr. Sahaja Akuthota[2], Mayukha Anumula[3]

Lingayas Vidyapeeth, Faridabad

Abstract: ***Cyber fraud presents a significant global challenge, with India facing similar issues. This phenomenon encompasses two primary dimensions: technological exploitation and psychological manipulation. Cybercriminals adeptly combine advanced technology with psychological tactics to deceive individuals, often resulting in substantial financial losses. Vulnerable individuals, particularly those experiencing mental health challenges, are frequently targeted, as fraudsters exploit their anxiety, emotions, fears, and depression to ensnare them in fraudulent schemes. Victims of cyber fraud span a wide range of socio - economic backgrounds, encompassing both educated and uneducated individuals. Fraudsters utilize cutting - edge technology and sophisticated psychological methods to deceive their targets, while many victims struggle to navigate the rapidly evolving technological landscape and innovative social engineering tactics. This study examines the dual aspects of cyber fraud—technological and psychological—and explores effective strategies to combat the increasing prevalence of cybercrime. The research is grounded in secondary sources, including academic papers, publications from the Reserve Bank of India, and documents from the Ministry of Home Affairs, Government of India. Additionally, the authors' expertise in cybersecurity and psychology enhances the depth of this investigation.***

Keywords: Cyber frauds, cyber crime, cyber security, psychology, technology, financial frauds, social engineering, honey traps, blackmail

1. Introduction

Over the past two decades, the world has witnessed remarkable advancements in technology, transforming various sectors and fundamentally altering how people live, work, and interact. One of the most significant developments has been the rapid growth of digital payment systems, which have revolutionized the global financial landscape. Digital transactions, such as online banking, mobile payments, and contactless transactions, have gained immense popularity, growing exponentially across many countries and making payments faster and more convenient than ever before.

In this global wave of digital transformation, India has emerged as a front - runner in adopting and implementing digital payment technologies. The country is setting new records each year, particularly in the realm of Unified Payment Interface (UPI) transactions, which have become widely accessible to people across urban and rural areas alike. This rapid adoption has contributed to India's financial inclusion efforts, enabling millions to participate in the digital economy and fostering greater economic growth.

However, alongside the tremendous growth in digital payments, there has also been a concerning rise in cyber fraud incidents in India. As the country's digital economy expands, so too do the risks associated with cybercrimes, such as identity theft, phishing, and financial scams. Cybercriminals are increasingly targeting digital payment platforms, exploiting technological vulnerabilities and often using sophisticated methods to deceive users and financial institutions. Consequently, as India continues to push toward a cashless economy, addressing these security challenges has become essential to safeguard the trust of consumers and to ensure the safe, reliable growth of digital transactions.

Cybercriminals are increasingly targeting a broad range of individuals by exploiting psychological tactics designed to manipulate and deceive. These criminals understand common human weaknesses, such as trust, fear, and curiosity, and use these insights to craft scams that play on emotions or create a sense of urgency. By sending convincing messages or posing as legitimate entities, cybercriminals are able to manipulate unsuspecting individuals into disclosing sensitive information, clicking on malicious links, or even authorizing fraudulent transactions. This strategic targeting isn't random but is often designed to appeal to vulnerabilities across different demographics, making it more likely that victims will fall for these schemes. In essence, cybercriminals are blending technology with psychology, creating scams that capitalize on human nature to achieve their malicious goals.

Cyber fraud encompasses various forms of deceit, such as phishing, identity theft, ransomware, financial scams, and data breaches, which target individuals, businesses, and institutions. Reports indicate that India ranks among the top countries experiencing high rates of cyber fraud, with cases steadily increasing in frequency and complexity. The economic impact is severe, costing millions in losses and undermining public confidence in digital systems.

This paper explores cyber fraud in India from two critical perspectives: the technological and the psychological. From a technological perspective, it examines the vulnerabilities in digital systems, gaps in cybersecurity infrastructure, and emerging technologies that both prevent and inadvertently facilitate cybercrime. The psychological dimension considers the cognitive biases, emotional triggers, and behavioural patterns exploited by cybercriminals to deceive and manipulate users. This dual approach provides a comprehensive understanding of how cyber fraud operates and spreads within a rapidly digitizing society.

Understanding the interplay of technological flaws and human psychology in cyber fraud is crucial for developing effective prevention and response strategies. By investigating these factors, this research aims to highlight key areas for intervention, offering insights for policymakers, financial institutions, cybersecurity professionals, and end - users on how to mitigate the risks associated with cyber fraud.

2. Literature Review

The rapid digitalization of India's economy, fuelled by initiatives like Digital India and the widespread adoption of smartphones and internet services, has unlocked unprecedented opportunities for individuals and businesses alike. From online banking and e - commerce to digital payments and social media, the digital landscape has become integral to the lives of millions of Indians. However, this digital transformation has also made users vulnerable to a range of cyber threats. Cyber frauds, in particular, have surged as malicious actors exploit both technological gaps and human vulnerabilities, presenting a significant challenge to cybersecurity frameworks in India.

Cyber fraud has been a focal area of research globally, with numerous studies highlighting the evolving nature of cyber threats and their impact on digital economies. In India, research on cyber fraud is relatively recent but rapidly growing as the digital economy expands and new vulnerabilities emerge. The literature on this topic broadly covers technological vulnerabilities, regulatory frameworks, and the psychological dimensions of cyber fraud, each of which sheds light on the multifaceted nature of cybercrime.

Overall, the existing literature reveals that while significant progress has been made in understanding cyber fraud from technological and psychological perspectives, there remains a need for integrated approaches that address both aspects simultaneously. This study aims to bridge these gaps by providing a comprehensive analysis that incorporates both technological and psychological factors, thereby contributing valuable insights for more effective strategies against cyber fraud in India.

There were numerous research studies across the globe on the challenge of cyber frauds, including India. A research study by Bruce, M. et al. (2024) [1], on global challenge of cyber frauds, reveals that Russia and Ukraine are prominent hubs for highly technical cyber frauds, while Nigerian cybercriminals typically engage in less sophisticated forms of cyber frauds. Some groups focus on moderately complex activities, such as data or identity theft, while others are involved in both advanced and simpler cyber offenses. Among these countries, India leans toward scams but maintains a balanced profile overall, whereas Romania and the USA show specialization in both technical and non - technical cyber frauds. The study by Chen, S. et al (2023) [2] finds that various factors, including high unemployment rates, limited legitimate economic opportunities, a widespread cybercrime subculture, weak cybercrime laws, and significant levels of corruption, drive individuals toward illicit wealth through cybercrime. Conversely, in high - income regions, cybercrime often arises in areas with a high Gini index and elevated education levels. A potential explanation is that highly educated individuals in these countries may receive lower compensation for their skills compared to their peers elsewhere, motivating them to turn to cybercrime as a means of enhancing their livelihoods. Indian Cyber Crime Coordination Centre (I4C), under the Ministry of Home Affairs has published a document titled "Cyber Hygiene for Cyber Space" containing a list of Do's and Don'ts for the citizens of the nation. According this publication (2022) [3], the rise of digital technology and internet usage has also led to an increase in cybercrime incidents. However, these can be managed or minimized through careful practices, precautions, awareness, and the use of effective security tools. The tips and recommendations in this document aim to help users keep their information, data, and devices secure.

According to the study by Kaur, M., et al (2017) [4], to combat cybercrime effectively, it is essential to create multidimensional collaborations between public and private sectors, including law enforcement agencies, the information technology industry, information security organizations, internet companies, and financial institutions. Unlike in the physical world, cybercriminals do not compete for dominance or control. Instead, they collaborate to enhance their skills and support each other in identifying new opportunities. Khan, S., et al (2022) [6] concluded in their study that in order to deal with global challenge of cybercrime, greater and more effective international cooperation is needed for evidence collection, information sharing, and the prosecution of those involved in cybercrimes. However, this can only be achieved if nations first incorporate substantive provisions into their legislation that criminalize cybercrimes. Analyzing the legal framework reveals more questions than answers, highlighting the undeniable need for constant adjustments and evolution in cybercrime legislation to keep pace with rapid and complex technical challenges. In recent Man - ki - Baat [5], Hon'ble Prime Minister Sri Narendra Modi urged every citizen of the nation to understand the huge challenge of growing Cyber Fraud cases including latest trend of "Digital Arrest" and shared three simple tricks "Ruko, Sacho, Action Lo", i. e. Stop acting in a hurry, think and then take action of reporting the cyber fraud to National Cyber Crime Reporting Helpline no: (telephone) 1930 or URL: https: //cybercrime. gov. in/. As per study by Mishra, S. & Panda, C. S. (2015) [7], self - awareness serves as a primary defense against cybercrime. Additionally, individuals can install firewalls to block many attacks and avoid installing unfamiliar software. This is important to raise awareness about potential threats and help people learn ways to protect themselves from these attacks.

Reserve Bank of India (2022) [8], published a booklet, titled "BE (A) WARE – Be Aware and Beware!" to educate the public on fraud prevention, particularly for those less familiar with digital financial transactions. Based on fraud incidents and complaints to RBI Ombudsmen, it provides practical advice on avoiding scams, emphasizing confidentiality of personal and financial information, vigilance with unknown communications, careful transaction practices, and regularly updating passwords and secure credentials. Reserve Bank of India (2021) [9], in its publication "*Raju and the Forty Thieves"* presented forty stories illustrating various fraud cases reported to the bank, including those from the RBI Ombudsmen and the Consumer Education and Protection Department (CEPD). Each story shares straightforward tips on precautions to prevent similar incidents. The character "Raju" represents an ordinary, trusting citizen, assuming various roles—such as a senior citizen, a farmer, or a carefree individual—to help readers from different backgrounds relate to him in various life situations. As per a research study by Saroja, A. & Radhika, R. (2018) [10], approximately 65% of bank - reported fraud cases involve technology - based crimes, such as those conducted via internet banking, ATMs,

and payment channels like debit, credit, and prepaid cards. Cyber frauds are highly technical in nature, making them difficult for law enforcement agencies to resolve. To effectively investigate these crimes, agencies need personnel with expertise in computer forensics.

Shah, R. (2019) [11], in his study, discusses various motivations behind cybercrimes, including financial gain, desire for fame, enjoyment, sexual exploitation, blackmail, business development, trafficking in illegal content, revenge, and pranks. A significant advantage for these criminals is their ability to operate online with relative anonymity, making them hard to trace. The global nature of the internet further complicates efforts by cyber officers and law enforcement, as crimes can occur anywhere in the world, and tracking such activities involves multiple locations, making it increasingly challenging to apprehend cybercriminals. In the research study by Subudhi, S & Pursani, P. (2024) [12], they concluded that to safeguard against financial fraud, individuals should stay informed and verify identities, use strong passwords along with two - factor authentication, and be cautious with unexpected communications. Protecting devices, securing Wi - Fi connections, regularly reviewing bank statements, thoroughly researching investments, and promptly reporting any suspicious activity are also key steps. Staying updated on scams and consulting legal advice when needed can further enhance protection. Talukdar, M. (2014) [13] discusses the various types of cyber crimes as Hacking, Virus/Trojans/Worms, Cyber Pornography, Cyber Stalking, Cyber Terrorism, Cyber Frauds, Phishing, Email Bombing, Email Spoofing, Salami Attack, Denial of Service (DoS) Attacks, Logic Bombs etc.

The terms **cyber crimes** and **cyber frauds** are often used interchangeably, but they have distinct meanings:

Cyber Crimes

Definition: Cyber crimes refer to illegal activities conducted via the internet or through computer systems. These can encompass a wide range of offenses.

Types:
- Hacking (unauthorized access to systems)
- Identity theft
- Cyberstalking
- Distribution of malware
- Online harassment
- Child exploitation
- Cyber terrorism

Cyber Frauds

Definition: Cyber frauds are a specific subset of cyber crimes that involve deceitful schemes aimed at financial gain or other benefits.

Types:
- Phishing (fraudulent emails to obtain sensitive information)
- Online scams (e. g., lottery scams, advance - fee fraud)
- Investment frauds
- Part time jobs/Work - from - Home Frauds
- Digital Arrest
- Google Search Frauds
- OLX Frauds
- Drugs in Courier Packet frauds
- Income tax refund frauds
- Bank account re - KYC frauds

Here's a comparison of cyber crimes and cyber frauds in a tabular format:

Aspect	Cyber Crimes	Cyber Frauds
Definition	Illegal activities conducted via the internet or computer systems.	Deceitful schemes aimed at financial gain or benefits.
Scope	Broad range of offenses (hacking, identity theft, etc.).	Specific subset focusing on financial deception.
Types	Hacking, cyberstalking, malware distribution, child exploitation, etc.	Phishing, online scams, investment frauds, credit card fraud.
Intent	Varies widely (malicious intent, political motives, etc.).	Primarily aimed at tricking victims for financial exploitation.
Examples	Cyber terrorism, online harassment, unauthorized data access.	Lottery scams, advance - fee fraud, auction fraud.

In cyber frauds, psychological manipulation plays a crucial role as fraudsters exploit human emotions and cognitive biases to deceive their victims. Here are some key psychological tactics they often use:

1) **Social Engineering and Trust Manipulation**: Fraudsters frequently employ social engineering tactics, where they build a sense of trust by posing as legitimate figures—such as bank officials, IT support staff, or even family members. This approach leverages the victim's tendency to trust authority figures or familiar personas, making it easier for the fraudster to extract sensitive information.
2) **Exploiting Urgency and Scarcity**: Many cyber scams, such as phishing emails, rely on creating a false sense of urgency or scarcity. Messages may imply that immediate action is necessary to avoid losing funds or missing out on a "limited - time offer. " This tactic leverages psychological principles related to loss aversion and scarcity, causing victims to act impulsively without fully verifying the legitimacy of the request.
3) **Emotional Appeals and Sympathy Triggers**: Some fraudsters evoke feelings of sympathy by fabricating distressing scenarios, like pretending to be a relative in an emergency or posing as someone in desperate need of financial assistance. By appealing to the victim's empathy, fraudsters manipulate emotional responses to overcome rational caution.
4) **Fear and Intimidation Tactics:** Cybercriminals sometimes use fear - based approaches, such as impersonating tax or law enforcement officials, to intimidate victims into compliance. Threats of fines, arrests, or lawsuits can provoke panic, leading victims to respond without assessing the legitimacy of the communication.

5) **Reciprocity Principle:** Some scams offer small gifts, discounts, or free services in exchange for personal information. This tactic leverages the psychological principle of reciprocity, where people feel obliged to return favours, thereby increasing the likelihood of sharing sensitive data.
6) **Authority Bias:** Impersonation of authoritative figures, such as government officials or bank executives, taps into authority bias, where individuals are more likely to comply with requests from perceived authority figures. Fraudsters exploit this bias by using official logos, formal language, and professional tones to appear credible.
7) **Playing on Financial Desires and Greed:** Many scams, such as investment frauds or lottery scams, play on individuals' desires for financial gain. By offering promises of easy money or significant returns, fraudsters exploit the victim's ambition or need for financial security, convincing them to overlook potential red flags.

By combining these psychological principles with digital tools, fraudsters create highly convincing schemes that target the emotional and cognitive vulnerabilities of victims.

3. Research Method

1) Research Design

This study adopts a qualitative research design to explore cyber frauds in India from both technological and psychological perspectives. The research aims to analyze the characteristics, trends, and impacts of cyber frauds, leveraging insights from secondary sources.

2) Data Sources

Secondary Data: The study primarily relies on secondary data collected from:

a) **Research Papers**: An extensive review of international and national journal articles that focus on cyber frauds, banking technology, and psychological aspects related to cyber frauds.
b) **Government Publications**: Reports and publications from reputable sources such as:
- Reserve Bank of India (RBI)
- Ministry of Home Affairs, Government of India

3) Data Collection Method

A systematic literature review approach will be employed to gather relevant research papers and publications. The following steps will be taken:

- **Database Search**: Utilize academic databases (e. g., Google Scholar, SciSpace, Dimensions. ai) to identify pertinent literature on cyber frauds.
- **Keyword Identification**: Use targeted keywords related to cyber frauds, banking technology, psychological perspectives, and related themes.
- **Selection Criteria**: Focus on peer - reviewed articles, official government reports, and authoritative publications that provide data on cyber frauds in India.

4) Data Analysis

The collected data will be analyzed using qualitative content analysis to identify key themes and patterns. The analysis will include:

- **Thematic Analysis**: Categorizing the findings based on technological factors (e. g., methods of cyber fraud, technological vulnerabilities) and psychological factors (e. g., victim behavior, fraudster psychology).
- **Comparative Analysis**: Comparing findings from different studies to draw comprehensive insights regarding the nature and prevalence of cyber frauds in India.

5) Integration of Author Experience

The authors' extensive backgrounds in banking technology and psychology will be integrated into the analysis, providing expert insights into the implications of the findings. This experiential knowledge will help contextualize the data and contribute to a deeper understanding of the psychological motivations behind cyber frauds and the technological measures that can mitigate these risks.

6) Limitations

The study recognizes that reliance on secondary data may limit the ability to draw definitive conclusions. Additionally, the rapidly evolving nature of cyber frauds necessitates continuous research to stay updated with emerging trends.

7) Conclusion

This research method aims to provide a comprehensive understanding of cyber frauds in India by examining both technological and psychological perspectives, thereby contributing valuable insights to policymakers, financial institutions, and researchers in the field.

4. Major Findings and Discussions

This section presents the key findings from the study "Cyber Frauds in India - An Investigation of Technological and Psychological Perspectives" and discusses their implications in light of the current landscape of cyber frauds in India.

1) Prevalence of Cyber Frauds

The analysis reveals a significant increase in cyber fraud incidents in India over the past few years. Data from various reports, including those published by the Reserve Bank of India, indicates that technology - based frauds account for approximately 65% of all reported fraud cases in the banking sector. This highlights the urgent need for enhanced cybersecurity measures to protect consumers and financial institutions.

2) Technological Vulnerabilities

The findings indicate that a majority of cyber frauds exploit specific technological vulnerabilities. Common methods include phishing attacks, malware infections, and ATM skimming. The study emphasizes that many of these attacks are facilitated by inadequate security protocols and outdated technology within financial institutions. This underscores the necessity for banks to adopt robust cybersecurity frameworks, including multi - factor authentication and advanced encryption methods, to mitigate these risks.

3) Psychological Aspects of Victimization

From a psychological perspective, the research identifies several factors that contribute to individuals falling victim to

cyber fraud. Cyber fraudsters exploit psychological manipulation to deceive victims, using tactics like:

a) **Social Engineering**: Building false trust by posing as authoritative or familiar figures, leading victims to share sensitive information.
b) **Urgency and Scarcity**: Creating pressure to act quickly with threats of lost opportunities or financial consequences, prompting impulsive actions.
c) **Emotional Appeals**: Evoking sympathy through fabricated distress scenarios to overcome the victim's caution.
d) **Fear and Intimidation**: Using threats from supposed officials to incite panic and compliance.
e) **Reciprocity Principle**: Offering small "gifts" to trigger a sense of obligation and prompt sharing of data.
f) **Authority Bias**: Exploiting the tendency to comply with authority figures by imitating officials and using formal tones.
g) **Financial Desire**: Promising easy money or investments to play on greed or financial needs, encouraging risky actions.

4) Impact of Awareness and Education

The research emphasizes the importance of awareness campaigns and educational programs in combating cyber frauds. Evidence suggests that individuals who participate in cybersecurity awareness initiatives are less likely to become victims. Implementing educational programs tailored to different demographic groups can empower individuals to recognize and respond to potential threats more effectively.

5) Role of Law Enforcement and Regulatory Bodies

The findings suggest that law enforcement agencies and regulatory bodies need to enhance their collaboration with financial institutions to tackle cyber frauds effectively. Currently, the fragmented approach to addressing cybercrime hinders timely response and investigation. A unified framework involving shared resources, training, and information exchange can strengthen the overall defense against cyber fraud.

6) Recommendations for Future Action

Based on the findings, the research proposes several recommendations:

- **Strengthening Cybersecurity Infrastructure**: Banks and financial institutions must invest in advanced technologies and continuously update their security measures to address emerging threats.
- **Psychological Profiling of Fraudsters**: Understanding the psychological motivations of cybercriminals can aid in developing targeted prevention strategies.
- **Community Engagement**: Building community partnerships to raise awareness about cyber frauds can foster a culture of vigilance and preparedness among consumers.

5. Recommendations

a) Enhancement of Cybersecurity Infrastructure:
- Financial institutions should invest in robust cybersecurity technologies, including advanced encryption, intrusion detection systems, and multi - factor authentication. Regular security audits and updates are essential to identify and address vulnerabilities proactively.

b) Comprehensive Cyber Awareness Programs:
- Implementing targeted awareness campaigns and educational programs can empower consumers, particularly vulnerable groups such as senior citizens and first - time internet users. These programs should cover topics such as identifying phishing attempts, safe online practices, and the importance of securing personal information.

c) Collaboration with Law Enforcement:
- Strengthening partnerships between financial institutions, law enforcement agencies, and regulatory bodies is crucial. A unified approach can facilitate timely reporting and investigation of cyber fraud incidents, thereby enhancing the overall response to cybercrime.

d) Psychological Profiling and Behavioural Insights:
- Utilizing psychological insights to understand the motivations and tactics of cybercriminals can inform preventive strategies. Financial institutions should develop training programs for employees to recognize suspicious behaviours and respond effectively.

e) Community Engagement Initiatives:
- Establishing community - based initiatives can foster a culture of vigilance and preparedness among consumers. Engaging local organizations, schools, and community centers can help disseminate information about cyber frauds and preventive measures.

f) Regulatory Framework Improvements:
- Policymakers should consider enhancing the regulatory framework surrounding cybersecurity practices in the financial sector. This could involve setting minimum security standards, mandatory reporting of cyber incidents, and establishing guidelines for best practices in cybersecurity.

6. Conclusion

The research study provides valuable insights into the complex landscape of cyber frauds in India. The findings reveal a significant rise in technology - based frauds, driven by both technological vulnerabilities and psychological manipulation. As cybercriminals become increasingly sophisticated, it is imperative for stakeholders—financial institutions, law enforcement agencies, and consumers—to adopt a proactive and collaborative approach to combat cyber frauds effectively. By enhancing cybersecurity measures, increasing public awareness, and fostering collaboration among relevant entities, the risk of cyber frauds can be significantly reduced. Moreover, understanding the psychological factors that contribute to victimization can aid in the development of more effective prevention strategies. This study underscores the urgent need for a multi - faceted approach to cybersecurity, emphasizing the importance of not only technological solutions but also the human element in preventing cyber frauds. By implementing the recommendations outlined in this research, stakeholders can

better protect consumers and contribute to a safer digital environment in India.

References

[1] Bruce, M., Lusthaus, J. T., Kashyap, R., Phair, N., Varese, F. (2024). Mapping the global geography of cybercrime with the World Cybercrime Index. *Plos One*. DOI: https: //doi. org/10.1371/journal. pone.0297312.

[2] Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., Guo, Q., Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. Humanities and Social Sciences Communications. https: //doi. org/10.1057/s41599 - 023 - 01560 - x.

[3] Indian Cyber Crime Coordination Centre (I4C), Government of India. (2022). Cyber Hygiene for Cyber Space - Dos and Don'ts – Basic Manual. URL: https: //i4c. mha. gov. in/theme/resources/Cyber%20Hygiene%20for%20Cyber%20Space%20 - %20Dos - Donts - Basic%20English%20Manual. pdf, Accessed on 25 - 10 - 2024

[4] Kaur, M., Kaur, G., Raina, C. K. (2017). Cyber Crime and Its Preventive Measures. International Journal of Advanced Research in Computer and Communication Engineering, Vol.6, Issue 3, DOI: 10.17148/IJARCCE.2017.63214

[5] Man Ki Baat (2024), Prime Minster's Man Ki Baath, Episode 115, URL: https: //www.youtube. com/watch?v=UUgR3U0qhY0, Accessed on 27 - 10 - 2024.

[6] Khan, S., Saleh, T., Dorasamy, M., Khan, N., Leng, OT. S., Vergara, R. G. (2022). A systematic literature review on cybercrime legislation. F1000Research 2022, 11: 971. https: //doi. org/10.12688/f1000research.123098.1

[7] MISHRA, S., PANDA, C. S. (2015). A Survey of Cyber Crimes. International Journal of Computer Science & Engineering Technology, Vol.6 No.12. Pg 650 - 654.

[8] Reserve Bank of India (2022). BE (A) WARE - A Booklet on Modus Operandi of Financial Fraudsters (URL: https: //rbi. org. in/commonman/english/Scripts/BEAWARE. aspx, Accessed on 26 - 10 - 2024)

[9] Reserve Bank of India (2021). Raju and the Forty Thieves – A Booklet on Modus Operandi of Financial Fraudsters, URL: https: //www.rbi. org. in/commonperson/English/Scripts/BasicBankingNew. aspx, Accessed on 25 - 10 - 2024.

[10] Saroja, A. & Radhika, R. (2018). A Study on Cyber Frauds in Indian Banking Sector. Asian Journal of Multi - Disciplinary Research, 4 (2): 57 - 62. DOI: http: //dx. doi. org/10.20468/ajmdr.2018.02.13

[11] Shah, R. (2019). Cyber Crimes in India: Trends and Prevention. *International Journal of Research and Analytical Reviews (IJRAR), 6* (1), 2348 - 1269.

[12] Subudhi, S. & Pursani, P. (2024). Financial Frauds – How to Alleviate Customer Grievances. *Bank Quest – The Journal of Indian Institute of Banking and Finance*. Vol 93, No.3. Pg - 24 - 33

[13] Talukdar, M. (2014). Cyber Crimes in India: A Study. International Journal of Research, Vol - 1, Issue - 10. Pg 891 - 905.