Digital Payment Frauds in India – Challenges and Solutions

Sri Rajashekara. N.
IPS & Research Scholar
School of Interdisciplinary and Tran disciplinary Studies Indira Gandhi National Open University, New Delhi, India 110068 E-mail rajashekarn1@yahoo.co.in (Corresponding Author)

Dr Abhishek Mishra
Assistant Professor
School of Interdisciplinary and Tran disciplinary Studies Indira Gandhi National Open University, New Delhi, India 110068, E-mail abhishekmishra@ignou.ac.in ORCID 0009-0008-3340-9749

Abstract: It is likely that every individual in India has encountered some form of cybercrime or fraud, even if they have not suffered a financial loss. Receiving a phishing email or text message qualifies one as a victim of cybercrime. The evolving tactics employed in digital payment fraud often involve requests for account numbers, usernames, or passwords under a Vishing Calls or sending the links to steal the credentials taking control of the Mobile devices. These days Digital Arrest, Fake Investment offers, Part time job frauds, QR scam codes, FedEx courier scams are on rise. The Modus Operandi changes but the anonymity of the fraudster using fake SIM cards, edited Aadhar card, using mule or rented bank accounts and the proceeds of the crime parked in Crypto almost remains almost the same.

Subsequently, Remote Access Trojans (RATs) such as TeamViewer or Any-Desk through phishing communications make the victims unwittingly grant control of their mobile devices to the perpetrators. In 2023, approximately 34% of users in India were targeted by local threats, positioning the country as the 80th most targeted globally. This ranking is derived from a report that examined the presence of malicious software directly on users' devices or on removable media connected to them, such as flash drives, memory cards, and external hard drives. The report also noted that many of these threats infiltrated systems through complex installers or encrypted files. Kaspersky products successfully blocked around 74,385,324 local incidents in India.

Key Words: Cybercrime, Digital Payment Fraud, Phishing, Cryptocurrency Fraud, and Remote Access Trojans (RATs)

Background: The cybersecurity market in India reached a valuation of USD 6.06 billion in 2023. Furthermore, nearly 67% of Indian enterprises are reportedly planning to outsource critical aspects of their security frameworks to manage the security service providers within next three years. With 560 million internet users, India ranks as the second-largest online market globally, following China. According to data from the National Crime Records Bureau (NCRB), there were 52,974 reported cases of cybercrime in India in 2021, reflecting a 5% increase from the 50,035 cases documented in 2020, and a 15% rise compared to previous years. There are 7000 Cyber Crimes happening every day not to mention large junk is unreported.

The rate of cybercrime rose from 3.3% of all registered criminal cases in 2019 to 3.7% in 2020. As reported by the National Crime Records Bureau (NCRB), the predominant type of cybercrime in 2020 was fraud, which constituted 60.2% of the total cybercrime cases, amounting to 30,142 out of 50,035 cases. Additionally, 6.6% of the cases, or 3,203 incidents, were related to sexual abuse, while 4.9%, equating to 2,440 cases, involved extortion. The NCRB also noted that there were 4,047 cases of online banking fraud in 2020, with 1,093 cases linked to OTP theft, 1,194 incidents of debit/credit card fraud, and 2,160 cases concerning ATM fraud. Furthermore, among the 578 cases of misinformation on social media, there were 972 cases of online harassment or cyberbullying targeting women and children, 149 cases involving fake profiles, and 98 cases related to data theft. In response to the growing cybercrime threat, the Cyber and Information Security (CIS) division was established in 2017, followed by the creation of the Indian Cyber Crime Coordination Centre (I4C) on January 10, 2020, under the Ministry of Home Affairs.

Cases Registered under Fraud for Cyber Crimes					
Credit/Debit cards	*ATMs*	*Online Banking frauds*	*OTP frauds*	*Others*	*Total*
1665	1690	6491	2910	4714	17470

Source: https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2080186

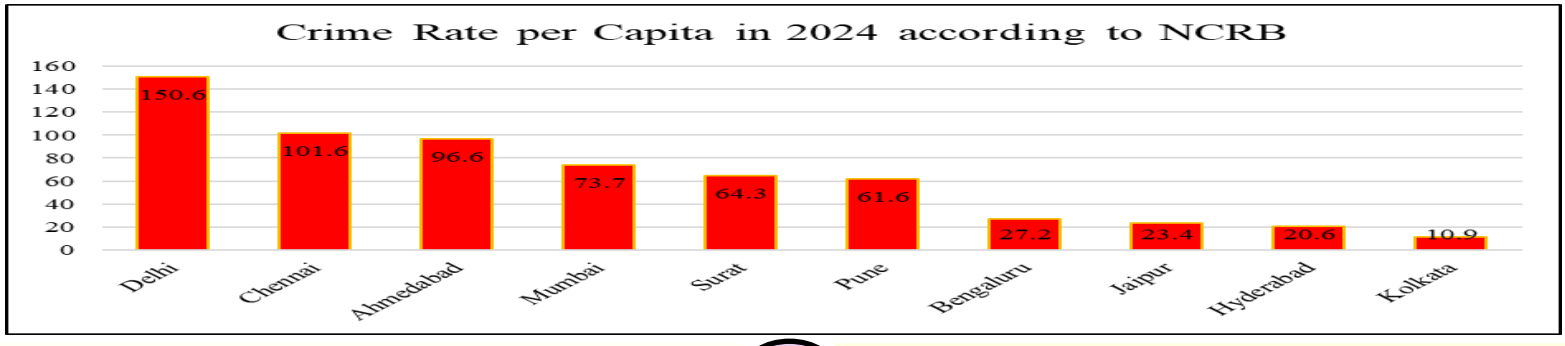
The National Cybercrime Forensic Laboratory, the National Cybercrime Training Centre, and the Joint Cybercrime Investigation Task Force are integral components of the cybercrime ecosystem management unit. Additionally, the National Cybercrime Research and Innovation Centre and the National Cybercrime Reporting Portal, along with the National Automated Fingerprint Identification System (NAFIS), were established on August 17, 2020. Furthermore, there exists a Registry of Foreigners involved in crime in India. Increasing Digital Payment frauds under financial frauds make the Ministry of Home Affairs come with separate wing of financial frauds under its portal National Cybercrime Reporting Portal. Further for Law Enforcement agencies www.Cyberpoliceportal.com has been established. Victim calling 1930 or registering under www.Cybercrime.gov.in can choose either financial frauds or the Cybercrimes against women and Children or other Cyber Crimes. If they prepare to go CEN police station (Cyber, Economic, Narcotics) then the Police will file a complaint under Police cyber portal.

Digital Payment Frauds in India: As for the latest statistics on cybercrime for 2023, the top five types of identity theft are as follows:

1. Credit card fraud (new accounts): 381,122 reports (42.0%)
2. Miscellaneous identity theft: 279,221 reports (30.7%)
3. Bank fraud (new accounts): 84,335 reports (9.3%)
4. Government benefits fraud (applied for/received): 82,419 reports (9.1%)

According to the annual report from the Reserve Bank, incidents of online payment fraud have surged fivefold in the financial year 2023-24, with cybercriminals defrauding individuals of Rs 14.57 billion (Rs 1457 crore) in the previous financial year. The Unified Payments Interface (UPI) service, launched in India eight years ago in 2016, has seen a remarkable increase in usage, with payments through UPI rising by 137 percent over the last two years. A record total of Rs 200 trillion has been transacted through UPI in India. The report indicates that the number of UPI transactions experienced a significant year-on-year growth of 56% in the second half of 2023, increasing from 42.09 billion to 65.77 billion. Concurrently, the value of transactions during this period surged by 44%, rising from INR 69.36 trillion to INR 99.68 trillion.

Challenges: The anonymity associated with individuals involved in digital payment fraud serves as a significant advantage for perpetrators. For instance, the SIM cards, PAN numbers, and identity documents they acquire are often counterfeit. A straightforward method for these fraudsters is to manipulate the Aadhar PDF copy, enabling them to obtain numerous SIM cards. The Centre for Development of Telematics (C-DOT), under the Government of India, utilizes ASTR software to identify the fake SIM using Facial recognition powered by Artificial Intelligence and Machine Learning using photographs used for SIM card applications. Each image is altered in various ways using Photoshop, and each Aadhar card undergoes multiple edits. Consequently, when the customer application forms are examined, they frequently lead to either unidentified individuals or non-existent entities. Retail outlets that provide SIM cards typically do not enforce stringent Know Your Customer (KYC) protocols, allowing them to distribute SIM cards for a nominal fee. Additionally, websites such as www.thispersondoesnotexist.com gives AI enable pictures of any individual. www.sms-receiver.com offer temporary SIM numbers to obtain OTP's from various countries, creating an ideal environment for fraudsters to establish fake accounts on different platforms, including social media. Channels on Telegram and Facebook, as well as WhatsApp groups, entice individuals with promises of high returns from cryptocurrency and stock market investments. Fraudsters, masquerading as investors, share messages claiming substantial profits within a short timeframe. Although the wallets may display impressive returns, actual withdrawals are consistently denied.



Source: https://www.indiatoday.in/technology/features/story/digital-arrest-scam-rising-in-india-here-is-how-to-protect-yourself-and-everything-else-you-need-to-know-2648746-2024-12-12

Solutions: The Government of India has established Know Your Customer (KYC) regulations for cryptocurrency investments. A 1% Tax Deducted at Source (TDS) is applicable on these investments, along with a 30% tax on profits derived from cryptocurrency trading, without the possibility of set-off or set-on, in contrast to the Goods and Services Tax (GST) framework. These regulations are designed to prevent the use of anonymous or fraudulent accounts in cryptocurrency transactions. Consequently, fraudsters have resorted to renting properties and creating rental agreements to alter the addresses on their Aadhaar cards. Using these modified local addresses, they open savings bank accounts to invest the illicit funds. They often disappear overnight, and when law enforcement requests address verification from Aadhaar, only the current address is provided, omitting any previous locations.

Cybercrime in India – Challenges: A significant limitation exists within the National Cyber Crime Reporting Portal (NCRP), which operates under www.cybercrime.gov.in. For instance, if individual A frauds individual B of ₹1 lakh, and B subsequently transfers ₹10,000 to ten different individuals, the NCRP may freeze the accounts of all ten beneficiaries. However, one beneficiary, C, may have received the funds legitimately for restaurant services, yet their account remains frozen. This situation has led to legal challenges for platforms like Wazir-X, which have been accused of handling funds that are deemed proceeds of crime.

Additionally, international digital payment frauds pose another challenge. For example, Chinese loan application scams often reroute funds to China through various currencies, which then appear as legitimate currency for the scam's accomplices in India. The recent digital arrest scam, where numerous Indians were held hostage in a cybercrime crisis, also involved multinational transactions, with currencies being converted through cryptocurrency investments. The new criminal laws have addressed issues of territorial jurisdiction, as the term "India" has been removed from Section 1 of the Bharatiya Nyaya Sanhita, allowing for the prosecution of digital payment frauds and cybercrimes on a global scale, including offenses committed using cryptocurrency.

Solutions: The term "India" has been incorporated into Section 1 of the Bharatiya Nyaya Sanhita (BNS), enabling the government to address digital payment fraud and cybercrimes on a global scale, particularly those involving cryptocurrencies, Virtual Private Networks (VPNs), Tor Onion browsers, and activities on the dark web and deep web. Section 48 of the BNS stipulates that abetting an offense committed outside India is now punishable, a shift from the previous provisions of the Indian Penal Code (IPC). Furthermore, Section 208 of the BNS clarifies that offenses registered in India can also pertain to actions committed outside the country. Cyber-crimes are encompassed under Section 111, which addresses organized crimes, while economic offenses, including hawala transactions and mass marketing fraud, fall under the same category. The definition of theft, as outlined in Section 112 concerning petty organized crimes, now includes thefts such as card skimming, shoplifting, and automated teller machine theft.

In relation to forgery, Section 337 of the BNS addresses the creation of counterfeit documents or electronic records, including identity documents issued by the government, such as voter identity cards and Aadhaar cards. The definition of theft of movable property has been broadened to include data theft and online theft through hacking of bank accounts or mobile cloning. Are we adequately prepared to combat the threat of digital payment fraud? While progress has been made, it remains insufficient. With the establishment of the Indian Cyber Crime Coordination Centre (I4C) and the introduction of Cyber Economic and Narcotics (CEN) police stations in each district, a framework is now in place to tackle these issues. However, the CEN police stations currently lack the necessary cyber forensics tools for effective investigations. It is imperative that our investigative officers enhance their capabilities to keep pace with the evolving tactics of fraudsters. A dedicated recruitment initiative for cyber specialists is essential at this juncture.High-value fraud cases are addressed through a mechanism where the lien amount refers to funds that are temporarily held. The cyber police portal allows law enforcement officers to submit requests, but only those involved in the criminal justice system are authorized to file complaints. Currently, there is coordination among all banks and the National Crime Records Bureau (NCRB). For instance, if a victim's account is with the State Bank of India (SBI), a police officer can file a complaint in the cyber police portal to trace the beneficiary.

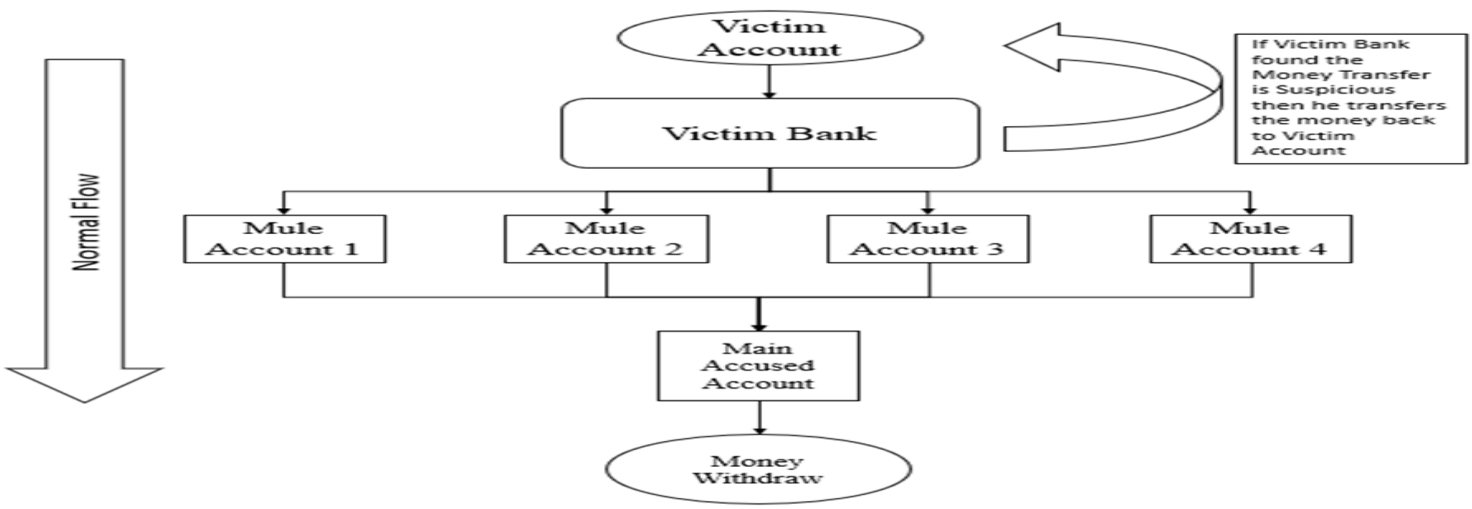
Most banks now have designated nodal officers responsible for managing payment-related issues. When a complaint arises regarding unauthorized debits or fraud, based on reports from law enforcement or the complainant, the next beneficiary is identified. If the funds have been utilized or transferred, this information is communicated to the relevant bank, complainant, or police officer. The integration of Artificial Intelligence is essential in tracing financial transactions,

determining the legitimacy of payments, and identifying potentially fraudulent activities, such as payments made for restaurant bills or purchases.

Banks operate customer care centres that handle such complaints promptly, available 24/7. Each bank has an incident manager stationed across the country, and two representatives from each bank are affiliated with the Indian Cyber Crime Coordination Centre. Furthermore, the all-India helpline number 1930 and the website www.cybercrime.gov.in have mapped nearly 14,000 police stations, ensuring that complaints can be directed to the appropriate local authorities.

The website www.cybercrime.gov.in or the helpline 1930 serves as a facilitative portal, directing complaints to either standard police stations or specialized Cyber, Economic, or Narcotics police stations. Each police station has designated state and district nodal officers responsible for addressing cyber-crimes and digital payment frauds. These nodal officers facilitate communication with relevant banks to trace KYC details and financial transactions. Upon receipt of a complaint, incident managers receive notifications in real-time.

For prompt resolution of grievances, the bank of the final beneficiary is authorized to transfer the fraudulent amount directly to the victim's account. For instance, if V is the victim's account and A, B, C, D, and E are intermediary accounts, the incident manager at bank E can directly credit the funds to V's account if the money is still available, bypassing the intermediary accounts. However, it is essential to maintain a mechanism that keeps these accounts and banks informed for future reference. Furthermore, the victim must obtain a court order through the relevant bank to establish that the funds in question are fraudulent and not legitimate payments. According to Section 457 of the Criminal Procedure Code (CrPC), a magistrate may issue orders for the return of property to the rightful owner if their identity cannot be determined, ensuring proper custody and handling of such property.



Police officers can trace the money trail and prevent further transfers through the Cyber Police portal, utilizing the authority granted under Section 149 of the CrPC, which empowers police to prevent cognizable offenses.

Currently, banks have raised concerns regarding complaints originating from the Cyber Police or the National Cyber Crime Portal. Such complaints are directed to the Grievance Redressal Officer of the respective state. If the Investigation Officer (IO) at the police station fails to take action within 30 days, the matter can be escalated to a senior officer, potentially of Deputy Inspector General (DIG) or Inspector General (IG) rank. The aggrieved party may also participate via video conferencing. The IO is required to submit the case within 10 days of receiving the complaint, as there is now an option for conducting a preliminary inquiry. However, in the realm of digital payments, complaints have already been lodged through various channels. Should the IO not act promptly, the senior officer can mandate specific actions within 48 hours.

Typically, fraudulent activities are linked to cryptocurrency investments. The 1% TDS applies to all investments, with a 30% tax on profits, devoid of set-off or set-on provisions. It is important to note that this framework is primarily a taxation measure rather than a regulatory one. Furthermore, from the previous financial year, individuals investing in the stock market are required to complete extensive income tax returns, which are quite detailed. The trading of cryptocurrency between sellers and purchasers occurs with minimal involvement of intermediaries, complicating the task for law enforcement to trace transactions. For instance, if an individual (A) transfers USDT in exchange for rupees from a victim's account, and the victim subsequently files a complaint, the victim's account may

be frozen to prevent further commission of a cognizable offense, given that funds have been diverted for cryptocurrency investment.

The Wazir-Ex platform has faced legal challenges due to KYC compliance issues, as it has not adequately verified whether investors are legitimate or if the funds received from them are derived from cyber fraud. The Government of India has established Know Your Customer (KYC) regulations for cryptocurrency investments. A 1% Tax Deducted at Source (TDS) applies to these investments, along with a 30% tax on profits generated from cryptocurrency trading, without the option for set-off or set-on, in contrast to the Goods and Services Tax (GST) framework. The Cyber Police portal has introduced several benefits, including a comprehensive format for submitting detailed information. However, the portal lacks user-friendliness, as completing all required fields can be time-consuming. Victims are expected to provide extensive documentation, such as screenshots of transactions and bank statements, which they may not readily have at hand. Additionally, individuals must possess a certain level of technological proficiency to utilize online banking applications, such as the SBI YONO app, to gather this information. This raises concerns for those who may not be as technologically adept, as they often resort to submitting brief complaints at police stations, which may not provide sufficient information for law enforcement to take action. It may be beneficial to implement a simplified complaint format on the portal to expedite the process.

Generally, the victims approach the bank when unauthorised payments made from their account. Banks check where the money gone and wash of their hands asking the victim to give complaint with the police. In North-eastern states the capacity of the investigation officers is not up to the mark, and they don't even collect the proper evidence. The crucial time has been elapsed to trace the money trail. Banking ombudsman in established across the country but hardly they could solve the digital payment frauds. Banks are not investigating agencies and only can provide the KYC and the creditor and debtor account details. Although the investigation methods are improved but only in few regions like South India, Delhi where the volume and the seriousness of the offences is more and has become a routine affair. The organised form of these crimes is threat. In Jamtaara, Mewad regions some villages, places and community as a whole is involved in Cyber Crimes.

I4C has a social media awareness handle called Cyber Dost where daily updates on Cyber frauds across the nation made known. Now most of the crimes are in always related to Cyber since use of Mobile, Internet is involved. But strictly the financial frauds and traditional crimes with usage of mobile are made separate categories.

Research Methodology:-

The research methodology for studying the rising threat of cybercrime in India and analyzing the effectiveness of current mitigation frameworks involves a mixed-method approach, combining both qualitative and quantitative techniques. The

methodology aims to provide a comprehensive understanding of the factors contributing to the growth of cybercrime, its impact on individuals and businesses, and the effectiveness of government and law enforcement interventions. The following steps outline the approach used for data collection, analysis, and conclusions.

1. **Data Collection**

Primary Data:

Surveys and Interviews: Primary data will be collected through surveys and structured interviews with individuals who have experienced cybercrime, as well as cybersecurity experts, law enforcement personnel, and financial institutions. These surveys will address the types of cybercrime incidents faced, including phishing, vishing, frauds involving digital payments, fake investment schemes, and more.

Victim Impact Assessment: Victims of cybercrimes, especially fraud, will be interviewed to understand the psychological, financial, and legal impact of the crimes. This will include the delays in grievance redressal and the effectiveness of existing mechanisms for reporting and resolving cybercrime cases.

Secondary Data:

Government Reports: Data from official sources such as the National Crime Records Bureau (NCRB), Kaspersky, and the Ministry of Home Affairs will be used to understand the scale and nature of cybercrime incidents in India. A key focus will be the 5% increase in cybercrime cases in 2021 and the 60.2% share of fraud cases within this rise.

Cybersecurity Industry Reports: Research reports from organizations like Kaspersky and other cybersecurity firms will be reviewed to examine the scope of local and global threats, such as the 34% of Indian users targeted by local threats in 2023 and the blocking of over 74 million incidents by Kaspersky in India.

Literature Review: Published academic papers, government policies, and global case studies on combating

cybercrime will be analysed to identify best practices and lessons learned from other countries.

2. Case Studies

Real-World Cybercrime Cases: Specific cybercrime incidents, including online banking fraud, vishing, QR code scams, fake investment offers, and remote access Trojan (RAT) attacks, will be examined in detail. Case studies will help illustrate the methods used by fraudsters, the vulnerabilities exploited, and the challenges faced by victims and law enforcement in addressing these crimes.

Government and Law Enforcement Initiatives: An analysis of initiatives like the Indian Cyber Crime Coordination Centre (I4C) and the establishment of Cyber and Information Security (CIS) will be conducted to assess the effectiveness of these frameworks in tackling cybercrime. The implementation of Know Your Customer (KYC) norms for cryptocurrencies, including taxation and reporting, will also be part of this assessment.

3. Data Analysis

Quantitative Analysis:

Cybercrime Statistics: The data collected from NCRB, Kaspersky, and other official sources will be analysed using statistical tools to track trends and patterns in cybercrime. This will include evaluating the rise in cybercrime cases, types of fraud, and geographical distribution of incidents. For example, the 5% annual increase in cybercrime cases and the 60.2% fraud rate will be used to analyse the prevalence of digital fraud.

Impact of Fraud: A detailed statistical breakdown will be performed on the types of frauds (such as online banking fraud, OTP theft, and card fraud) and the correlation between digital payment adoption and rising cybercrime.

Qualitative Analysis:

Victim and Expert Insights: The qualitative data from surveys and interviews will be analyzed thematically to identify common challenges faced by cybercrime victims, such as delays in grievance redressal, lack of cyber forensic tools, and limited technological expertise in rural areas. The responses from law enforcement and cybersecurity experts will also be analyzed to assess the gaps in the current legal and technical frameworks.

Modus Operandi of Fraudsters: The study will also identify recurring patterns in the methods employed by cybercriminals, such as the use of fake SIM cards, edited Aadhaar cards, mule accounts, and cryptocurrency for laundering the proceeds of fraud.

Analysis

1. Trends in Cybercrime

Rising Incidence of Digital Fraud: The analysis will focus on the growing trend of cybercrime in India, with particular emphasis on digital payment frauds, fake investment schemes, QR code scams, and remote access Trojan attacks. The research will examine how fraudsters have adapted their tactics over time, leveraging technologies such as fake SIM cards, counterfeit identity documents, and cryptocurrency to evade detection.

Geographic Distribution: A breakdown of cybercrime cases by state and region will be performed, focusing on urban versus rural disparities. Particular attention will be given to the challenges faced in rural areas where there may be less technological awareness and access to cybersecurity resources.

2. Government and Law Enforcement Response

Effectiveness of Cybersecurity Frameworks: The analysis will assess the effectiveness of the Indian Cyber Crime Coordination Centre (I4C), the Cyber and Information Security division (CIS), and the legal frameworks established for cryptocurrency regulation. The success of initiatives like the Know Your Customer (KYC) for cryptocurrencies and the introduction of taxes (1% TDS and 30% profit tax) will be analysed.

Challenges in Law Enforcement: The study will evaluate the challenges faced by law enforcement agencies in investigating and prosecuting cybercrime cases. This will include a focus on the limited availability of cyber forensic tools, the lack of trained personnel, and the delays in grievance redressal processes that contribute to the persistence of cybercrime.

3. Victim Support and Grievance Redressal

Impact on Victims: The analysis will examine the psychological, financial, and emotional toll of cybercrime on victims, particularly focusing on the long and often inefficient grievance redressal process. The delay in resolving complaints and the victim's experience with law enforcement agencies and financial institutions will be critically assessed.

Improvement of Redressal Mechanisms: Recommendations for improving grievance

redressal mechanisms will be explored. This may include enhancing the accessibility and efficiency of complaint platforms, streamlining procedures, and increasing victim support services.

4. Recommendations

Based on the findings, the study will propose measures to enhance India's cybersecurity landscape. Recommendations will focus on improving law enforcement capabilities, the need for advanced cyber forensic tools, increasing the number of trained cyber specialists, and refining the grievance redressal process for cybercrime victims. Additionally, the research will suggest policy improvements for better coordination between banks, law enforcement, and cybersecurity firms.

Through this mixed-method approach, the study will provide a detailed analysis of the current state of cybercrime in India, assess the effectiveness of government and law enforcement responses, and offer actionable recommendations to mitigate the rising threat of cybercrime.

Conclusion: Cybercrime in India is rising exponentially, impacting individuals across the country, with fraudsters employing tactics such as phishing, vishing calls, remote access tools, QR code scams, and fake investment schemes. Digital payment frauds often leverage fake SIMs, counterfeit Aadhaar cards, mule accounts, and cryptocurrency to obscure identities. In 2023, India ranked 80th globally for cyber threats, with Kaspersky blocking over 74 million local incidents. Cybercrime cases rose by 5% in 2021, with fraud constituting 60.2% of cases, while identity theft, card skimming, and misinformation continue to escalate. The Government of India has implemented frameworks such as the Indian Cyber Crime Coordination Centre (I4C), CEN police stations, and Know Your Customer (KYC) regulations for cryptocurrencies, including a 1% TDS and 30% tax on profits. However, law enforcement struggles with a lack of cyber forensic tools, delayed investigations, and limited technological expertise, particularly in rural areas. While banks coordinate with law enforcement to trace fraudulent transactions, victims often face prolonged grievance redressal processes. To combat digital fraud effectively, it is essential to enhance investigative capabilities, recruit cyber specialists, and streamline complaint mechanisms through user-friendly platforms.

****

References:

1. https://www.business-standard.com/india-news/here-is-how-much-indians-lost-to-cyber-frauds-between-jan-and-apr-of-2024-124052700151_1.html
2. https://www.statista.com/statistics/1499739/india-cyber-crime-cases-reported-to-i4c/
3. https://economictimes.indiatimes.com/news/india/indians-lost-over-1750-crore-to-cyber-fraud-in-first-four-months-of-2024/articleshow/110444616.cms
4. A comprehensive survey of cybercrimes in India over the last decade (https://ijsra.net/sites/default/files/IJSRA-2024-1919.pdf)
5. https://bytescare.com/blog/punishment-for-plagiarism-in-india
6. https://www.statista.com/topics/5054/cyber-crime-in-india/
7. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2080186
8. https://economictimes.indiatimes.com/news/india/bns-vs-ipc-how-bhartiya-nyay-sanhita-is-different-from-old-ipc-law-legal-experts-break-down-the-nitty-gritties-of-some-key-changes/articleshow/111408786.cms?from=mdr
9. https://www.reuters.com/world/india/india-cenbank-governor-pushes-stronger-governance-cybersecurity-banks-2024-07-03/
10. https://nypost.com/2024/05/17/business/two-chinese-nationals-arrested-in-73m-pig-butchering-crypto-scam/
11. https://koinly.io/guides/crypto-tax-india/
12. https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf
13. https://nyayasanhita.schoolnxg.com/bills/Bhartiya_Nagrik_Suraksha_Sanhita_2023/Chapters/Chapter_XIV/Sections/Section_208/index.html
14. https://devgan.in/bns/section/48/