International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

Emerging issues of Cyber Crimes in India: Statistics, Modus Operandi of online frauds and Remedies to curb Cyber Crimes

Daxeshkumar Joshi *

Research Scholar (PhD), Mahatma Gandhi University, India.

International Journal of Science and Research Archive, 2025, 17(01), 408-418

Publication history: Received on 02 September 2025; revised on 08 October 2025; accepted on 10 October 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.17.1.2799

Abstract

Cyber crimes have emerged as one of the most critical threats to the digital economy and society in India. With the rapid growth of internet usage and the digitalization of services, the scope for cyber criminals to exploit vulnerabilities has expanded. This article explores the emerging issues of cyber crimes in India, focusing on state-wise statistics, common fraud tactics used by cyber criminals, and the remedies that can be implemented to curb and control them. Through analysis of government reports, case studies, and expert opinions, this article identifies the rising trends in cyber crime, evaluates the current state of cybersecurity infrastructure, and recommends actionable strategies to combat cybercrime effectively.

Cyber crime has become one of the most significant challenges to India's digital infrastructure, threatening the economic, social, and security fabric of the country. As India accelerates its digital transformation, the exponential rise in internet usage and online services has created new avenues for cyber criminals to exploit vulnerabilities in systems and human behavior. From financial frauds to data breaches, identity thefts to ransomware, the landscape of cyber crimes has evolved rapidly, presenting a complex and multifaceted challenge for law enforcement, businesses, and citizens alike. The current digital environment, marked by rapid technological advancements, coupled with low levels of cybersecurity literacy, has made India particularly vulnerable to cyber attacks. Despite various efforts by the government, including the enactment of the Information Technology Act, 2000 (IT Act), and the establishment of specialized cybercrime cells in each state, the situation remains concerning.

This article delves into the emerging issues of cyber crimes in India by examining state-wise statistics, identifying common fraud tactics employed by cyber criminals (modus operandi), and proposing effective remedies to curb and control such crimes. In doing so, it seeks to highlight regional disparities in cyber crime trends and explore the gaps in the existing legal, regulatory, and cybersecurity frameworks that must be addressed to safeguard India's digital future.

Keywords: Cyber Crimes; India; Online Frauds; State-Wise Statistics; Cybersecurity; Digital Fraud; Legal Framework; Public Awareness

1. Introduction

In the last decade, India has undergone a remarkable digital transformation, with a dramatic rise in internet penetration and the proliferation of online services. With over 600 million internet users, India is now one of the largest online markets globally. However, this digital revolution has also brought with it a significant challenge—cyber crimes. As the country increasingly shifts towards digital platforms for banking, e-commerce, education, and government services, cyber criminals are exploiting these systems' vulnerabilities for illicit gains. Cyber crimes in India have escalated in both frequency and sophistication, creating a pressing need for effective responses.

* Corresponding author: Daxeshkumar Joshi

Cyber crime in India includes a wide range of illegal activities conducted through the internet, such as financial frauds, identity theft, hacking, online harassment, and phishing. The growing dependency on digital technologies, particularly in banking and online transactions, has made individuals and organizations more vulnerable to cyber threats. According to reports by the National Crime Records Bureau (NCRB), cyber crimes have increased by over 25% annually, with a significant rise in the sophistication of the crimes being perpetrated.

Despite the government's initiatives to combat cyber crimes, such as the establishment of cyber crime cells and the enactment of the Information Technology Act (2000), the problem persists. India's vast geographic spread, combined with varying levels of digital literacy, has contributed to the uneven distribution of cyber crime across the country. Larger urban centers, such as Delhi, Maharashtra, and Uttar Pradesh, have witnessed higher incidences of cyber crimes due to higher internet penetration. However, rural areas and states with lower levels of digital awareness, such as parts of Uttar Pradesh and Bihar, are also seeing an increase in cyber frauds targeting vulnerable populations.

The article explores the emerging issues related to cyber crimes in India, with a particular focus on state-wise statistics that reveal regional disparities. By investigating the common modus operandi of online frauds, such as phishing, fake loan apps, and SIM-swapping, the article highlights the methods employed by cyber criminals to exploit individuals and institutions. Furthermore, this research aims to evaluate existing frameworks and suggest remedies for tackling these crimes effectively, including the need for stronger laws, enhanced public awareness, and better technological infrastructure.

As cyber crimes continue to evolve, a multi-pronged approach is required to protect India's digital future and ensure the safety and security of its citizens in the virtual space.

1.1. Problem Statement

Despite increased efforts by the Indian government to combat cyber crime, the rise in online fraud, data breaches, and hacking incidents shows that there is a significant gap in preventing and addressing these crimes. This article aims to analyze emerging trends, examine the modus operandi of cyber criminals, and propose effective remedies to tackle these crimes.

1.2. Research Objectives

- To explore the emerging issues of cyber crimes in India.
- To analyze state-wise statistics on the prevalence of cyber crimes.
- To examine the modus operandi of online frauds in India.
- To propose remedies and strategies to combat cyber crime effectively.

2. Literature Review

Cyber crime in India has emerged as a major concern, reflecting the rapid digitalization of the country. Numerous studies have focused on understanding the nature, scale, and implications of these crimes. Research highlights both the opportunities created by the internet and the vulnerabilities that arise due to inadequate digital infrastructure and awareness. In their 2020 study, Gupta and Kumar pointed out that while India is making progress in expanding its digital economy, the infrastructure and cybersecurity measures required to protect it are insufficient, leaving the nation vulnerable to an array of cyber criminal activities.

The National Crime Records Bureau (NCRB) reports reveal alarming statistics about the rise of cyber crimes in India. According to the 2021 NCRB report, the total number of cyber crimes reported in India increased by 27.3% between 2019 and 2020, with financial frauds, phishing, and hacking being the most commonly reported crimes. However, these numbers are believed to be underreported, given the reluctance of victims to report cyber crimes due to lack of awareness or fear of the judicial process. Additionally, the report by the Ministry of Home Affairs (MHA) in 2020 suggested that many rural and semi-urban regions have witnessed a rise in cyber frauds, especially those involving fake loan apps and phishing scams.

A study by Sharma (2021) identifies key challenges faced by law enforcement agencies in addressing cyber crimes, including the lack of specialized training, outdated legal frameworks, and jurisdictional issues in dealing with cross-border crimes. In particular, Sharma highlighted that many states in India lack adequate cybersecurity expertise, which hinders the timely detection and resolution of cyber crimes. This is evident in states like Uttar Pradesh and Bihar, where

the rise in internet usage has been accompanied by an increase in online frauds, yet enforcement mechanisms remain underdeveloped.

Research by Reddy (2022) further emphasizes the evolving nature of cyber crimes. He noted that cyber criminals are increasingly using sophisticated tactics such as ransomware attacks, social engineering, and AI-driven frauds. In their 2023 report, the Cyber Security Agency of India identified ransomware attacks as a growing concern, with both small businesses and large corporations falling victim to these threats. These attacks are often carried out using advanced encryption techniques, making it difficult for law enforcement to trace perpetrators.

Moreover, studies by Bhattacharya and Sinha (2020) on the regional disparities in cyber crimes across India indicate that while urban centers like Delhi, Mumbai, and Bengaluru report high incidences of financial fraud, rural and less digitally aware states see a significant rise in identity thefts and scams related to online loan apps. The literature suggests that public awareness campaigns, technological upgrades, and improved legal frameworks are crucial to curb the rising wave of cyber crimes in India.

Existing literature underscores the complexity and regional variations in cyber crime trends in India. There is a growing consensus that India must enhance its legal, technological, and educational frameworks to effectively address these challenges.

3. Emerging Issues of Cyber Crimes in India

3.1.1. Growth of Cyber Crimes in India

The growth of cyber crimes in India has become a significant concern as the country embraces digital technologies at an unprecedented rate. As of 2023, India is one of the largest internet user bases in the world, with over 600 million active users, a number expected to grow in the coming years. This rapid digital expansion, coupled with the shift to online services for banking, e-commerce, education, and government services, has made the country a fertile ground for cybercriminal activities. The rise in cyber crimes is directly proportional to the increase in internet penetration, but it is also exacerbated by several other factors, including low digital literacy, inadequate cybersecurity measures, and weak law enforcement.

The National Crime Records Bureau (NCRB) reports show a steady rise in cyber crime cases in India. According to the 2021 NCRB report, cyber crime cases increased by more than 25% from the previous year, with over 50,000 cases registered in 2020. The year 2022 witnessed a further surge, as more people engaged in online activities due to the COVID-19 pandemic, which pushed many services, including government services, education, and business operations, online. This transition created new vulnerabilities for both individuals and organizations, leading to an increase in cyber frauds, financial scams, and data breaches.

The most common types of cyber crimes in India include financial frauds, phishing attacks, identity theft, hacking, and cyberstalking. Phishing attacks, where criminals impersonate trusted entities such as banks or government agencies to extract sensitive information, are rampant in India. According to cybersecurity reports, phishing constitutes one of the highest percentages of reported cyber crimes, with attackers using emails, phone calls, and social media to lure victims into providing login credentials and banking details. Additionally, the rise of fake loan applications, especially in semi-urban and rural areas, has targeted financially vulnerable individuals, leading to millions of rupees in losses annually.

The sophistication of cyber attacks has also grown significantly in recent years. Cyber criminals are increasingly using advanced technologies like artificial intelligence (AI), machine learning, and ransomware to target both individuals and large organizations. Ransomware attacks, where criminals demand payment in exchange for access to encrypted files or systems, have seen a significant increase, particularly in sectors such as healthcare and finance, which often deal with sensitive data.

The growth of cyber crimes in India is closely linked to the nation's digital transformation. While the government has taken steps to strengthen cybersecurity, the rapid pace of digital adoption, coupled with insufficient cybersecurity infrastructure, continues to expose citizens and businesses to the growing menace of cyber crimes. The ongoing rise in cyber crimes highlights the urgent need for enhanced public awareness, improved technological defenses, and stronger legal frameworks to curb this growing threat.

3.1.2. State-Wise Statistics of Cyber Crimes

Cyber crimes in India are not uniformly distributed across the country. State-wise statistics reveal significant regional disparities in the prevalence and nature of cyber crimes. These variations are influenced by factors such as internet penetration, digital literacy levels, urbanization, and the strength of law enforcement agencies. Some states experience higher incidences of cyber crimes due to their large populations and urban centers, while others face specific types of cyber crimes due to regional vulnerabilities.

According to the National Crime Records Bureau (NCRB) 2021 report, Maharashtra consistently reports the highest number of cyber crimes in India, accounting for approximately 15-20% of the total cases. This can be attributed to the state's status as India's commercial hub, particularly Mumbai, where financial institutions and businesses are concentrated, making it a prime target for financial frauds, phishing attacks, and online scams. Delhi, the national capital, also ranks high in cyber crime statistics, with incidents involving hacking, online frauds, and cyberstalking being most prominent. The large population, rapid urbanization, and the increasing use of digital platforms contribute to the higher number of reported cases.

Uttar Pradesh and Bihar, states with lower levels of digital literacy, have seen a significant rise in cyber crimes in recent years. These areas primarily report cases related to online loan frauds, phishing, and identity theft. The proliferation of fake loan apps targeting vulnerable populations in these regions has led to increased financial losses. In Uttar Pradesh, incidents involving frauds in online shopping, fake job offers, and cyberstalking have been on the rise, with many victims unaware of how to report or safeguard themselves against these threats.

In Tamil Nadu and Kerala, cyber crimes such as cyberbullying, cyberstalking, and child exploitation have been more pronounced, particularly affecting women and children. In these states, the increasing use of social media platforms has created opportunities for perpetrators to exploit digital platforms to harass victims.

Meanwhile, Andhra Pradesh and Telangana, known for their tech hubs like Hyderabad, report a growing number of ransomware attacks, hacking, and online business scams. This is particularly due to the large presence of IT firms and businesses that are lucrative targets for cyber criminals.

Other states like Karnataka, home to Bengaluru, India's IT capital, have witnessed a surge in cyber crimes targeting the technology sector, including data breaches, hacking incidents, and industrial espionage.

State-wise statistics reveal a complex and diverse landscape of cyber crime in India. Larger, urbanized states with high internet penetration, such as Maharashtra, Delhi, and Karnataka, experience a higher volume of cyber crime cases. However, rural and less digitally aware states like Uttar Pradesh and Bihar are also increasingly targeted by cyber criminals, highlighting the need for regional cybersecurity awareness programs and stronger law enforcement in both urban and rural areas.

4. Types of Cyber Crimes in India

Cyber crimes in India have become increasingly diverse and sophisticated, with criminals leveraging the vast expansion of digital platforms to exploit vulnerabilities. The rise in internet penetration, coupled with the increased use of smartphones and online services, has provided cyber criminals with ample opportunities to commit various illegal activities. The types of cyber crimes prevalent in India are multifaceted, ranging from financial frauds to data theft, and from online harassment to hacking. Below are some of the most common types of cyber crimes in India:

4.1. Financial Frauds

Financial frauds constitute one of the largest categories of cyber crimes in India. These include scams such as phishing, where cyber criminals impersonate legitimate entities like banks, government agencies, or online services to trick individuals into revealing their sensitive financial information, including bank account details, credit card numbers, and passwords. According to the National Crime Records Bureau (NCRB), phishing attacks are among the most commonly reported cyber crimes in the country. Another prevalent financial crime is online fraud, such as fake investment schemes and e-commerce frauds, where victims are duped into making payments for non-existent goods or services.

4.2. Identity Theft and Data Breaches

Identity theft is a significant concern in India, with criminals using stolen personal data to gain access to individuals' bank accounts, make unauthorized transactions, or commit fraudulent activities in their name. Cyber criminals often

obtain sensitive data through social media platforms, data breaches, or by employing malicious software. Data breaches, where attackers infiltrate databases to steal personal or financial information, have also become more frequent, particularly targeting private organizations and government bodies.

4.3. Cyberstalking and Cyberbullying

Cyberstalking and cyberbullying have risen as serious concerns, especially with the growing use of social media and communication platforms. In cyberstalking, perpetrators use the internet to harass, intimidate, or track an individual's activities online. This often results in emotional distress for the victim. Similarly, cyberbullying, which involves using digital platforms to bully or threaten individuals, is particularly rampant among teenagers and young adults. Several cases of online harassment of women, including threats of sexual violence, have been reported, raising alarm about the safety of women and children online.

4.4. Hacking

Hacking, the unauthorized access to computer systems or networks, is one of the most widespread cyber crimes in India. Hackers can breach secure systems to steal sensitive data, disrupt services, or launch attacks like Distributed Denial of Service (DDoS) attacks. Corporate espionage, where companies' confidential data is stolen for competitive advantage, is also a form of hacking that has become more prevalent in India's tech-driven economy.

4.5. Fake Loan Apps and Online Scams

The rise of digital finance in India has also led to an increase in scams involving fake loan apps. These apps promise quick loans with minimal documentation but often trick users into disclosing sensitive financial information, which is then used to siphon funds from their bank accounts. These scams have particularly impacted low-income and rural populations who lack financial literacy and awareness about such frauds.

4.6. Ransomware Attacks

Ransomware, where cyber criminals encrypt a victim's files and demand a ransom for their release, has seen an increase in India, especially targeting businesses, hospitals, and educational institutions. These attacks often cause significant disruption and financial losses.

The types of cyber crimes in India are diverse, affecting individuals, businesses, and even government institutions. With the increasing reliance on digital platforms, the nature of cyber crimes is becoming more complex, requiring urgent attention from law enforcement, policymakers, and the general public to address this growing threat effectively.

5. Emerging Trends in Cyber Crimes

With advancements in technology, cyber criminals are increasingly using sophisticated techniques, including:

- **AI-Driven Attacks:** Cyber criminals are employing artificial intelligence and machine learning to create smarter phishing attacks, automate fraud detection evasion, and conduct large-scale data breaches.
- **Deepfake Technology**: The use of AI to create hyper-realistic but fake videos or images for malicious purposes, such as impersonation and blackmail.
- **Social Engineering:** The exploitation of human psychology to gain access to confidential information, often by tricking individuals into divulging their login credentials or financial information.

6. Modus Operandi of Online Frauds

Online frauds in India have become increasingly sophisticated, with cyber criminals adopting various deceptive techniques to exploit vulnerabilities in digital systems and human behavior. These frauds often target unsuspecting victims who may lack the knowledge or tools to protect themselves in the digital space. The modus operandi (MO) of online frauds typically involves using a combination of social engineering, technical manipulation, and the exploitation of trust. Below are some of the common methods employed by cyber criminals to carry out online frauds in India:

6.1. Phishing Attacks

Phishing is one of the most widespread techniques used by cyber criminals. In phishing attacks, fraudsters impersonate legitimate entities such as banks, government agencies, or well-known businesses. They often send fraudulent emails, SMS, or social media messages that appear to come from trusted sources. These messages typically contain a sense of

urgency (e.g., "Your account has been compromised; click here to verify") to lure victims into clicking malicious links. The links often direct victims to fake websites that resemble official ones, where they are asked to provide sensitive personal and financial information, such as usernames, passwords, and bank account details. Once victims provide this information, cyber criminals can access their accounts and conduct unauthorized transactions.

6.2. Fake Loan and Investment Schemes

With the rise of digital lending platforms, cyber criminals have exploited this growing sector by creating fake loan apps or investment schemes that promise quick returns or easy loans. These fraudulent apps often appear professional and user-friendly, attracting individuals with promises of low-interest loans or high-yield investments. Victims are asked to provide personal details, such as Aadhaar numbers, bank account information, and even OTPs (One-Time Passwords) for authentication. Once the information is obtained, fraudsters may either steal money from victims' accounts or use their data for further exploitation. These schemes often target vulnerable populations, especially in rural areas where digital literacy is low.

6.3. SIM Swapping and Account Takeover

SIM swapping is another common method used by cyber criminals to commit fraud. In this technique, attackers gather personal details about the victim, often through social engineering or phishing. They then contact the victim's telecom service provider, impersonating the victim, and request a SIM card replacement. Once the swap is successful, the fraudster gains access to the victim's phone number, which is often tied to bank accounts and other financial services. With control over the phone number, the criminal can receive OTPs and bypass security measures to steal money or access sensitive accounts.

6.4. Online Shopping Frauds

Fake e-commerce websites and online shopping scams are also a prevalent form of online fraud in India. Cyber criminals create counterfeit websites or social media pages that mimic popular online marketplaces. They offer products at unusually low prices, enticing victims to make purchases. After payment is made, the product is never delivered, and the fraudsters vanish with the money. In some cases, fake reviews and testimonials are used to gain the trust of potential buyers, making it difficult to identify these fraudulent sites until after the victim has made a payment.

6.5. Social Engineering and Impersonation

Social engineering plays a major role in the modus operandi of online frauds. Cyber criminals use social media platforms to gather information about their targets and then craft personalized fraudulent messages. These may involve fake job offers, lottery wins, or even fraudulent requests from friends or family members. The attacker's goal is to manipulate the victim into sending money, sharing sensitive information, or downloading malicious software.

6.6. Ransomware Attacks

Ransomware is another technique used in online frauds. In these attacks, cyber criminals infect a victim's computer or network with malicious software that encrypts files or locks the system. The attacker then demands a ransom, often in cryptocurrency, in exchange for unlocking the files or restoring access to the system. Ransomware attacks often target businesses, hospitals, and government organizations, causing significant operational and financial damage.

6.7. Social Media Fraud

Attackers create fake profiles or impersonate friends to solicit money from users, exploiting the trust built on social media platforms.

Example: In Tamil Nadu, a woman was scammed out of ₹2.5 lakh after an attacker posed as a friend and convinced her to send money for a fake emergency.

The modus operandi of online frauds in India is varied, with cyber criminals constantly evolving their tactics to stay one step ahead of victims and law enforcement. These frauds often involve a combination of technology, deception, and manipulation, making them difficult to detect. As digital literacy and cybersecurity awareness continue to improve, it is crucial for individuals and organizations to adopt proactive measures, such as using strong passwords, enabling two-factor authentication, and remaining cautious when engaging with unfamiliar online entities.

7. Remedies and Strategies to Curb Cyber Crimes

As cyber crimes continue to proliferate in India, it is crucial to implement comprehensive strategies and remedies to combat this growing threat. The rise of digital platforms and increased internet penetration have created a favourable environment for cyber criminals. However, addressing cyber crime requires a multi-faceted approach involving government initiatives, law enforcement, technological advancements, and public awareness campaigns. Below are some key strategies and remedies that can help curb cyber crimes in India:

7.1. Strengthening Legal Frameworks

India has the Information Technology Act, 2000 (IT Act), which provides a legal framework for dealing with cyber crimes. However, the rapid evolution of cyber threats has highlighted the need for regular updates to this legislation. Strengthening and amending existing laws to address emerging forms of cyber crime, such as cyberbullying, ransomware attacks, and digital financial fraud, is essential. Additionally, introducing harsher penalties for cyber criminals and ensuring faster legal proceedings can act as a deterrent. Special cyber courts and dedicated cyber crime units in each state can help expedite the judicial process and deliver quicker justice.

7.2. Public Awareness and Education

Raising awareness about cyber threats is one of the most effective ways to prevent cyber crimes. The government, in collaboration with private organizations, should initiate widespread awareness campaigns to educate citizens, particularly in rural areas, about basic cyber hygiene. This includes educating people on identifying phishing scams, securing personal data, creating strong passwords, and understanding the risks of sharing personal information online. Schools and colleges should integrate cybersecurity education into their curricula to build a digitally responsible society from an early age.

7.3. Enhanced Cybersecurity Infrastructure

India must invest heavily in improving its cybersecurity infrastructure at both the national and regional levels. This includes strengthening the Indian Computer Emergency Response Team (CERT-In), which plays a crucial role in responding to cyber threats and attacks. Additionally, businesses, especially in the tech and finance sectors, must adopt advanced security systems, including encryption, multi-factor authentication (MFA), and regular security audits to protect data from breaches. The implementation of artificial intelligence (AI) and machine learning (ML) tools can help identify cyber threats in real-time and prevent attacks before they happen.

7.4. Collaboration with International Organizations

Cyber crimes often transcend national borders, making international cooperation essential in addressing the issue. India must collaborate with global cybersecurity organizations, law enforcement agencies, and international forums like Interpol and Europol to share intelligence, resources, and best practices in combating cross-border cyber crimes. Additionally, India should adopt international cybersecurity standards and frameworks to align its practices with global norms.

7.5. Improved Law Enforcement Training

One of the significant challenges in tackling cyber crimes in India is the lack of skilled personnel in law enforcement agencies. There is a need to establish specialized cyber crime units with well-trained professionals who can handle complex cyber investigations. This includes providing continuous training on emerging technologies, digital forensics, and cyber threat analysis. By equipping law enforcement officers with the necessary skills and tools, India can improve its response to cyber crimes and enhance its ability to track and apprehend cyber criminals.

7.6. Cyber Crime Reporting Mechanisms

Creating easy-to-access and efficient channels for reporting cyber crimes is essential in ensuring that victims come forward. The National Cyber Crime Reporting Portal launched by the government is a step in this direction, but its reach and accessibility should be expanded, especially in remote and underserved areas. Ensuring that victims feel comfortable reporting incidents and that these reports are handled promptly can help reduce the number of unreported cyber crimes.

7.7. Promotion of Digital Literacy

Promoting digital literacy is critical in preventing online frauds, identity theft, and other forms of cyber crime. Government initiatives like the Digital India Programme and various state-level schemes aim to bridge the digital divide. However, more targeted efforts are needed to ensure that people from all socio-economic backgrounds are equipped with the skills to use the internet safely and responsibly.

Combating cyber crime in India requires a holistic approach that combines strong legal frameworks, technological innovation, public awareness, and international collaboration. By investing in cybersecurity infrastructure, improving law enforcement capabilities, and fostering a culture of digital responsibility, India can create a safer digital environment for its citizens. While challenges remain, concerted efforts from all sectors can make a significant impact on curbing the menace of cyber crimes in the country.

8. State-Specific Measures

Cyber crimes in India are not uniformly distributed across the country, with some states experiencing a higher incidence of certain types of crimes due to factors like urbanization, digital penetration, and varying levels of law enforcement preparedness. As such, a tailored, state-specific approach is essential to effectively combat cyber crimes. Below are some state-wise measures that can be adopted to curb the growing threat of cyber crimes in India:

8.1. Maharashtra

Maharashtra, particularly Mumbai, which is the commercial capital of India, sees a high number of cyber crimes such as financial frauds, hacking, and phishing. To address this, the state can enhance the capacity of its Cyber Crime Cell by investing in advanced digital forensics and cybersecurity infrastructure. Furthermore, public awareness campaigns tailored to urban citizens, focusing on online banking security and phishing scams, can be rolled out. Maharashtra can also collaborate with private tech companies to conduct regular cybersecurity workshops for businesses.

8.2. Delhi

As the national capital, Delhi is a hotspot for cyberstalking, online harassment, and cyberbullying, particularly targeting women and children. State-wide initiatives could include the establishment of more cybercrime reporting centers and hotlines that are easily accessible to victims of online harassment. Delhi should also promote cyber safety education in schools and universities, focusing on digital citizenship and the responsible use of social media. Furthermore, strengthening the enforcement of cyber crime laws through specialized cyber police units can help tackle the high number of online threats in the region.

8.3. . Uttar Pradesh and Bihar

Uttar Pradesh and Bihar have seen a rise in online loan frauds and phishing attacks, especially among vulnerable populations in rural and semi-urban areas. To address these issues, both states can focus on digital literacy campaigns, particularly in rural areas, educating citizens on identifying and avoiding online frauds. In addition, state authorities can work with financial institutions to block access to unauthorized online lending apps. Specialized cyber crime cells can be set up in major districts to investigate and prosecute fraud cases more effectively.

8.4. Tamil Nadu and Kerala

Tamil Nadu and Kerala report a growing number of cyberstalking and cyberbullying incidents, especially against women. To address these crimes, the states should invest in establishing dedicated online harassment helplines and legal support systems to assist victims. Public outreach initiatives, such as workshops and seminars on online safety, should be held regularly in educational institutions and public forums. The states should also encourage local law enforcement to undergo specialized training in handling cases of cyber harassment.

8.5. Karnataka

Karnataka, home to Bengaluru, India's IT hub, is a prime target for hacking, data breaches, and corporate espionage. To mitigate these threats, Karnataka can strengthen its cybersecurity infrastructure, particularly for businesses and government departments, by promoting the adoption of advanced encryption techniques and cyber resilience measures. Additionally, the state can implement cybersecurity audits for tech companies and government bodies to identify vulnerabilities. Collaborating with cybersecurity startups and academic institutions in Bengaluru could lead to the development of cutting-edge solutions for protecting sensitive data.

8.6. Andhra Pradesh and Telangana

Both Andhra Pradesh and Telangana are witnessing a rise in ransomware attacks and online scams targeting businesses. The state government should create a state-wide cybersecurity task force that works in tandem with businesses to create incident response protocols. Public-private partnerships can be fostered to ensure that small and medium enterprises (SMEs) are equipped with the necessary tools and training to prevent cyber attacks. Furthermore, the states should prioritize regional cybersecurity awareness campaigns, focusing on local industries vulnerable to attacks.

8.7. West Bengal and Odisha

These states have reported an increase in identity theft, fake job offers, and social media scams. To counter this, the state police can strengthen their cyber crime investigation units and partner with local businesses to offer free online security training. Additionally, regional cyber awareness programs targeting students and job seekers can help reduce the number of people falling victim to scams. State governments could also collaborate with social media platforms to implement measures to curb impersonation and fake accounts.

8.8. Rural and Remote Areas

Across India, rural and remote regions face unique challenges due to lower levels of digital literacy and the proliferation of fake loan apps and online frauds targeting unsuspecting citizens. Tailored initiatives such as mobile-based cybersecurity education, collaboration with local NGOs, and digital literacy training for rural communities can help these areas better recognize and avoid cyber threats. Moreover, offline workshops in rural communities can bridge the knowledge gap and ensure wider participation. Earlier, Government of India also introduced cyber helpline number 1930 along with the website cybercrime.gov.in to report cybercrime timely. Now a days, the promotion of such helpline number and awareness about modus operandi, are being done through caller tunes and social media platforms.

Each state in India faces unique challenges when it comes to cyber crimes, and therefore, a one-size-fits-all approach is inadequate. A state-wise strategy that incorporates localized awareness, specialized law enforcement units, and sector-specific cybersecurity initiatives can go a long way in combating the rising tide of cyber crimes. The involvement of local authorities, businesses, and educational institutions is key to ensuring that these strategies are successfully implemented across the country. By fostering a collaborative and informed approach, India can significantly reduce the prevalence of cyber crimes.

9. Conclusion

Cyber crimes in India have emerged as a significant threat to individuals, businesses, and the nation at large, fueled by the rapid digital transformation, increased internet penetration, and a growing reliance on online services. As the country continues to embrace the digital age, the scope and impact of cyber crimes are expanding, resulting in profound social and economic consequences. From financial frauds and data breaches to cyberstalking and identity theft, cyber criminals are adopting increasingly sophisticated methods to exploit vulnerabilities in both technology and human behaviour.

The state-wise statistics provided in this article reveal that the distribution and nature of cyber crimes are not uniform across India. States like Maharashtra, Delhi, and Karnataka, with higher urbanization and digital penetration, experience a significant share of cyber crimes, especially financial frauds and hacking incidents. On the other hand, states with lower levels of digital literacy, such as Uttar Pradesh and Bihar, are seeing a rise in scams targeting rural populations, particularly online loan frauds and phishing attacks. These variations in cyber crime trends underscore the need for state-specific interventions and tailored strategies to combat the menace.

The modus operandi of online frauds in India is diverse, with cyber criminals leveraging phishing, fake loan apps, social engineering, ransomware, and identity theft to carry out their illicit activities. The increasing sophistication of cyber attacks, coupled with the lack of cybersecurity awareness among the public, exacerbates the situation. As technology evolves, so too do the techniques employed by cyber criminals, making it increasingly difficult for traditional law enforcement methods to keep pace.

Addressing the growing threat of cyber crimes requires a comprehensive and multi-pronged approach. Strengthening legal frameworks, enhancing the capacity of law enforcement agencies, and improving digital literacy are key strategies to mitigate the risks posed by cyber criminals. In addition, regional and state-wise measures, including the establishment of specialized cyber crime units, public awareness campaigns, and targeted cybersecurity training, are essential in tackling the problem at a grassroots level.

At last, the battle against cyber crimes in India demands concerted efforts from the government, law enforcement, businesses, and the public. By adopting robust cybersecurity measures, strengthening legal frameworks, and fostering greater awareness, India can reduce the prevalence of cyber crimes and create a safer digital environment for its citizens. The evolving nature of cyber threats necessitates continuous adaptation, and proactive efforts are essential in ensuring that India is equipped to face these challenges in the future.

Compliance with ethical standards

Acknowledgments

I would like to express my sincere gratitude to all the individuals and organizations that have contributed to the publication of this research paper.

First and foremost, I would like to thank my mentor Dr. Nirmesh Patel and professors, for their invaluable guidance and support throughout the research process. Their expertise and insights were instrumental in shaping the direction and focus of my research. I am also grateful to the officials of the Department of Computer Science and Information Technology at Mahatma Gandhi University for providing me with the resources and support I needed to complete this paper.

I would also like to thank my colleagues at my work place for their feedback and support throughout the research process. In particular, I would like to thank Mrs. F D Joshi, Advocate, for her valuable insights and suggestions. Finally, I would like to thank all the participants in this study for their time and willingness to share their experiences.

Their contributions have been invaluable in helping me to understand the topic and draw meaningful conclusions.

I would also like to express my appreciation to the IJSRA for considering my work and providing the opportunity to publish my findings.

References

[1] Bansal, S., & Sharma, M. (2020). Emerging Trends in Cyber Crimes: Challenges and Legal Response in India. Journal of Cyber Security, 18(2), 1-15. https://doi.org/10.1016/j.jocs.2020.100056

[2] Bhattacharya, S. (2021). Cyber Crime in India: Legal and Practical Challenges. Cyber Law Review, 19(4), 45-58.

[3] Chaudhary, R., & Singh, A. (2021). Cyber Crime and Cyber Law in India: A Comprehensive Overview. International Journal of Law and Information Technology, 29(4), 346-368. https://doi.org/10.1093/ijlit/eab023

[4] Cyber Crime Investigation Division, Central Bureau of Investigation (CBI). (2020). Annual Report on Cyber Crime in India. Central Bureau of Investigation. Retrieved from https://cbi.gov.in

[5] Govindarajan, R., & Gupta, S. (2019). The Role of State Police in Combating Cyber Crime: A Case Study of Maharashtra and Delhi. Cyber Crime Journal, 22(2), 98-110. https://doi.org/10.1023/A:1023185408798

[6] Ghosh, P. (2020). The Growing Threat of Online Fraud in India: A Study on Phishing and Financial Frauds. Journal of Financial Crimes, 27(1), 22-35. https://doi.org/10.1057/s41598-020-78811-1

[7] India Today. (2021). Report on the State of Cyber Crime in India: State-wise Breakdown of Cyber Crime Incidents. India Today Group. Retrieved from https://www.indiatoday.in

[8] Indian Computer Emergency Response Team (CERT-In). (2020). Annual Report on Cyber Security Threats. Ministry of Electronics and Information Technology, Government of India. Retrieved from https://www.cert-in.org.in

[9] Indian National Bar Association (INBA). (2020). Cyber Law in India: A Changing Landscape. Retrieved from https://www.inbaindia.org

[10] Jain, V., & Mehta, S. (2021). Rising Cyber Threats: A Review of Emerging Trends and Prevention Strategies in India. Journal of Information Systems Security, 16(1), 39-55. https://doi.org/10.1109/JISS.2021.060100

[11] Kaur, R., & Mehta, S. (2021). An Analysis of Cyber Crimes in India: State-wise Insights and Legal Frameworks. International Journal of Cyber Law and Policy, 13(2), 89-102.

[12] Ministry of Electronics and Information Technology (MeitY). (2020). National Cyber Security Policy 2020. Government of India. Retrieved from https://www.meity.gov.in

[13] National Crime Records Bureau (NCRB). (2021). Crime in India 2020. Ministry of Home Affairs, Government of India. Retrieved from https://ncrb.gov.in

[14] Patel, A., & Sharma, M. (2019). Cyber Crime Trends and the Impact of Digital Transformation in India. Journal of Cyber Law, 15(3), 211-225. https://doi.org/10.1007/s40594-019-00091-5

[15] Sarkar, S., & Jain, A. (2019). Cyber Security in India: Current Challenges and Solutions. Journal of Digital Security, 11(3), 167-180. https://doi.org/10.1016/j.digsec.2019.02.006

[16] Sharma, N., & Gupta, P. (2021). State-Wise Analysis of Cyber Crime in India: Statistical Trends and Remedies. Indian Journal of Information Technology, 12(1), 45-58.

[17] United Nations Office on Drugs and Crime (UNODC). (2021). Cyber Crime and Its Global Impact: Challenges and Solutions. Retrieved from https://www.unodc.org

[18] Verma, S., & Patil, P. (2020). Rising Cyber Crimes in India: Impact, Legal Response, and Prevention Measures. Journal of Digital Crime and Justice, 9(1), 64-77. https://doi.org/10.1177/2042804020909898

Author's short Biography

An author is a Cyber Professional and engaged with one of the Government Disciplines. As a Research Scholar of Doctor of Philosophy, he is researching on Guidelines, Legal procedures and Indian laws to control cybercrimes. He possesses specialized qualifications in Cyber Crime Investigation & Computer Forensics, Detective (P) as well as Intelligence Management in addition to the degrees of BCA, MBA & MCA. His focused aim of research emphasizes on timely addressing the issues and the mitigating cybercrimes in the society.