Journal of Applied Social Sciences and Humanities

https://journal.krrishpub.com/index.php/jassh/index

RESEARCH ARTICLE

Growing Incidence of Cybercrime in India: Causes and Remedies

Abhay Bora [a,*], Gayatri N Nayak [b], Prem Kulsrestha [c]

[a] *Sandip Institute of Technology and Research Centre (SITRC), Nashik- 422 213, India.*
[b] *Thakur College of Engineering & Technology, Thakur Village- 400 101, Mumbai, India.*
[c] *Savitribai Phule Pune University, Ganeshkhind, Pune- 411 007, India.*

Abstract

Over the last ten years, India's digital transformation has dramatically altered its social and economic landscape. At the same time as providing unparalleled opportunity for economic development, it has exposed the Indian population to rapidly emerging and intensifying levels of cybercrime. This study explores the growing prevalence of cybercrime within India using official data from the National Crime Records Bureau (NCRB) and the Indian Cyber Crime Coordination Center (I4C). It will examine the multi-faceted dimensions of this issue. The research aims to identify key factors contributing to the dramatic rise in cybercrimes, assess how effective are current institutional frameworks for managing cybercrime, and propose actionable policy options based on empirical data for enhancing prevention of and prosecutions for cybercrimes. Two main hypotheses were tested by this study. Hypothesis 1 states that the growth in cybercrime offenses is directly related to increases in Internet penetration throughout India. Hypothesis 2 states that, despite enactment of the Information Technology Act 2008 and establishment of the I4C mechanism, these have not resulted in reductions in cybercrime offense growth rates. The methodology employed for conducting the analysis was documentary analysis. Registered cybercrime offenses increased at an annualized rate of approximately 35.5% during 2014-24. Offense numbers rose from 9622 in 2014 to 86,420 in 2023. In addition, registered offense numbers rose to 101,928 in 2024, an increase of nearly 18%. Therefore, substantial shortcomings exist regarding mechanisms for recovering lost funds. The low conviction rate of just 2.6% in 2023 demonstrates that there are serious deficiencies in the criminal justice system which prevent effective prosecution of cybercrime offenders. Both of the above stated hypotheses have been supported by the results of this study. The study concluded with specific and actionable recommendations for enhancing India's cybersecurity infrastructure and for improvement of prosecution outcomes for cybercrimes.

Keywords: Cybercrime, Digital fraud, I4C, NCRB, Internet penetration, Conviction deficit.

Article information:
ISSN: 3139-4892 (Online)
Published by: **Krrish Scientific Publications Pvt. Ltd.**
DOI: https://doi.org/10.71426/jassh.v2.i1.pp73-88
Received: *20 Apr. 2026* | Revised: *11 Jun. 2026* | Accepted: *20 Jun. 2026* | Published: *24 Jun. 2026*

1. Introduction

The large-scale transformation of India's socioeconomic profile, with respect to the use of digital technologies and their influence on individual and collective well-being, has created a myriad of problems for both governments and businesses. The Digital India Initiative was developed to provide digital solutions to various issues affecting India such as poverty, illiteracy, unemployment and poor health care. The initiative has resulted in nearly 900 million people accessing digital services such as e-banking, e-healthcare, e-governance and e-learning. Since launching the Digital India initiative in 2015, India has become one of the fastest-growing Internet markets globally. As at 1st April 2024, India has 954.4 million active internet users. The country has also seen a tremendous increase in the amount of money being spent using mobile payments. For example, since the launch of UPI (Unified Payments Interface) in 2016, it has grown to account for 81% of all digital transaction volume in the fiscal year 2024-25 [6], making India one of the countries moving furthest toward becoming a completely cashless economy. Despite this success, there is another side to the story of India's digital revolution. With increasing numbers of people accessing the Internet comes an increase in the amount of cybercrime occurring

*Corresponding author
Email addresses: drabhaybora@gmail.com (Abhay Bora), gayatri.nayak@sbup.edu.in, gayatrinayak1606@gmail.com (Gayatri N Nayak), premkulsrestha@gmail.com (Prem Kulsrestha).

within India. Cybercrime is growing faster than digital usage. There were fewer than 10 thousand cybercrimes reported in 2014 compared to nearly 87 thousand reported in 2023 [1]. The number of cybercrimes reported in 2024 was greater than 101 thousand showing a yearly increase of 31.2%. These numbers show a relationship between increased digital activity and an increase in cybercrimes. It is therefore reasonable to say that as Indians continue to get more connected to the Internet, they will become more vulnerable to cybercrime. India's connection to the Internet is creating new opportunities for criminals. Criminals can easily target thousands of people using just one email. Therefore, it would seem logical for authorities to take proactive steps to prevent cybercrimes. Unfortunately, many of those who experience cybercrimes do not report them due to lack of knowledge about how to report crimes, fear of being judged negatively because they lost money or other reasons [19]. Cybercrime affects not only individuals but also the government and businesses. The primary motivation behind cybercrime is financial gain. In fact, financial-related cybercrime accounted for 72.6% of all cybercrimes committed in 2024. Therefore, we see a massive negative impact on the overall economy of India due to cybercrime. Additionally, India is potentially facing threats from foreign hackers that could lead to more severe consequences for the country [23]. As mentioned earlier, there is a high percentage of unreported cybercrime cases. The low conviction rate also reflects poorly upon the ability of the criminal justice system to successfully investigate and prosecute cases involving cybercrime. The low conviction rate of only 2.6% for cases brought before courts in 2023 shows that the Indian legal system is failing to adequately deter cybercrime. A major reason why cybercrime continues to grow rapidly in India is due to lack of effective legislation and laws to deal with cyber offenses. Although India passed the Information Technology Act 2000 as amended in 2008 to create a regulatory body for dealing with cybercrimes, many scholars argue that this act lacks clear definitions of what constitutes cyber offenses, clarity on jurisdictions, and procedures for collecting electronic evidence [16], [18]. Also, although the Indian Government established the Indian Cyber Crime Coordination Center (I4C) in 2019-20 with the goal of providing a centralized platform for states and central agencies to collaborate on investigating cybercrimes, reports indicate that cybercrime incidents continue to rise after the center became operational [3]. Thus, we need to evaluate the effectiveness of such institutional innovations like I4C. The unique characteristics of the cyber environment require special strategies for controlling digital crime. Jurisdictional ambiguity, anonymity and rapid technological changes are some of the factors that make it difficult to develop an effective strategy for preventing digital crimes [31], [39]. Hence, we cannot assume that institutions that exist today can handle the needs of tomorrow. Based on our previous discussions on the scope of cybercrime in India, nature of cybercrime, institutional responses and gaps in existing laws and regulations, this study aims to achieve three interrelated goals. First, we aim to analyze the time series data of registered cybercrime cases in India during 2014-2024 and examine if there exists a correlation between the rate of increase in registered cybercrime cases and the corresponding rate of increase in internet users [2]. Second, we intend to assess whether or not the existing laws/legislations (IT Amendment Act 2008 and I4C) implemented by Indian authorities have been able to reduce the rate of increase in cybercrime cases or improve the rate of convictions [42]. Thirdly, we want to assess if these existing laws/legislations have been effective enough in reducing cybercrime. To pursue these goals we will test two hypotheses. Hypothesis one (Hypothesis One - H1) assumes that there is a positive correlation between the rate of increase in registered cybercrime cases in India and the corresponding rate of increase in internet users [2], [11], [12]. The rationale behind hypothesis one is based on Routine Activity Theory which explains that the rate of crime increases when motivated offenders face suitable targets with little presence of guardians [11] ,[12]. Similarly, hypothesis two (Hypothesis Two - H2) assumes that the implementation of I4C (2019-20) and related legislations have failed to produce a statistically significant decrease in growth rates of cybercrime, similarly, a conviction rate less than three percent indicates an institutional failure to deter cyber offenders [42], [16], [18].

2. Review of literature

2.1. The trajectory of cybercrime growth in india

The rapid development of cybercrime in India is currently the biggest governance challenge for the Internet age. Data collected from official government sources show a trend that can't be easily explained as a linear progression, instead, there's been an extremely fast increase that exceeds the ability of institutions to respond. Statistics provided by the National Crime Records Bureau indicate the number of registered cybercrimes in India grew exponentially from 9,622 in 2014 to 86,420 in 2023. That is a near-eight fold rise of around 800% during a period of almost ten years. The numbers clearly demonstrate that cybercrime not only increased significantly on an overall basis but that it became a larger portion of total crimes due to increasing usage of computers and other technologies (as measured by the crime rate rising from 2.1 to 7.3 per lakh population) . The year 2024 will mark another major development when the number of reported incidents exceeded the one-lakh barrier and reached 1,01,928 recorded offenses – a level many researchers attribute to the growing availability of online services, greater knowledge of technology among those who are exposed to cybercrime risks, and ever-improving criminal methods at large-scale operation [9], [10]. The interpretation of these growth rates should be done carefully because some researchers say there is an overestimation in reported increases of cybercrime due to changes in the way data is reported (not necessarily increases in crime). Formalizing the process of registering cybercrimes, establishing specialized police units for cybercrime and increasing public education will result in statistically inflating cybercrime trends making it difficult to analyze trends directly [10], [12]. In addition to the above considerations, the increase in cybercrime observed has shown a significant variation across different categories of measured crime that cannot be solely explained by changes in reporting practices. Institutional

research into the patterns of growth of cybercrime indicate that even though technology development first creates opportunities for offenders, the correlation between the use of digital technologies and victimization are non-linear and depend on many factors including the regulatory environment, law enforcement capability and social-cultural context [9], [11]. From this perspective, India's growth pattern is characteristic of countries experiencing rapidly developing digital markets, immature regulatory frameworks and disadvantages for victims in terms of their ability to exploit international cyber space as compared to potential offenders [10], [12].

2.2. Internet penetration and the volume of opportunity

The structural framework of growth of cybercrimes in India is built on the greatest expansion in history of internet accessibility and digital consumer behavior. By March 2024 there were 954.4 million Internet Subscribers (Telecom Regulatory Authority of India), accounting for about 67% of India's total population and making it one of the biggest online communities around the world [2]. The average monthly data use was at 25.7 Gigabyte per Subscriber (Telecom Regulatory Authority of India) by 2025, not only are people passively connected to the Internet through this level of access, they actively engage with Data-Intensive Applications & Services that require high levels of bandwidth [2]. The number of transactions processed by the Unified Payment Interface (UPI) is an actual measure of the size and growth trend of India's Digital Financial Ecosystem. In terms of transactions per year, they grew from 4,370 crore in the first year to 16,443 crore in the last year with a nearly four-fold increase which represents a reflection of both success in terms of the acceptance rate and increasingly digital nature of economy-wide activities [6]. Researchers who are examining how digital connection impacts rates of cybercrime victimization have found that payment platforms provide especially vulnerable environments for victims of cybercrimes. This vulnerability can be attributed to factors such as the speed at which payment platforms operate, the degree of anonymity associated with use of many platforms and the lack of clear jurisdictional authority on each platform resulting in environments that favour fraud [17], [18]. The rapid growth of payment platforms has correspondingly increased the potential "attack surfaces" for malicious users, creating what researchers call opportunity volume effects where the larger amount of legitimate uses of these platforms result in proportionally larger amounts of opportunities for criminals [9], [11], [20]. The relationship between Internet penetration and the incidence of cybercrime has become increasingly a topic of interest for researchers in comparative criminology. Comparative research across criminological contexts indicates that the positive correlation found in many studies between wealth and technological advancement is contingent upon the level of institutional development, where high connectivity levels are present in a society there may be multiple relationships between digital risk (or "exposure"), enforcement capacity, and societal trust which can result in higher than expected or lower than expected cybercrime incidence levels [9], [10].

2.3. Digital literacy and the reporting paradox

Data regarding cybercrime case reports across different areas of India has shown an apparent disconnect from expected relationships between digital proficiency and the likelihood of victimization. While Karnataka is typically ranked as being amongst India's most digitally literate and technologically advanced States, it was also responsible for recording the highest number of cybercrime cases – 21,889 in 2023 – contradicting expected results where increased digital literacy could result in greater awareness of how to protect oneself online. Furthermore, while West Bengal is one of the lower reporting States (309 cybercrime cases in 2023) , this State contains sizeable urban populations who have similar levels of access to technology as those found in other parts of the country [1], [5]. There are a number of theoretical models from research into digital literacy and cybercrime reporting to explain why there is such an inverse relationship in the data. Researchers indicate that higher levels of technical ability can create both increased (protective) and decreased (exposure to new ways to be attacked, knowledge of what types of attacks need to formally reported as crimes) opportunities for individuals who engage in crime at their own peril [44], [45], [47]. Individuals with higher levels of literacy report that they have a better understanding of how to identify fraudulent schemes, keep evidence of those frauds and find ways to report them when required, these factors produce statistically significant results that confound the distinction between being a victim of crime versus the propensity to report a crime [48], [56]. Studies based upon data collected by National Statistical Offices on education level show that engagement in technology creates numerous opportunity paths, while creating some avenues for protection against crime through developing the individual's digital competency, it also expands the target space of potential attacks [5], [50], [57]. Cybercrime Reporting Paradox demonstrates a difference between Cybercrime Visibility & Cybercrime Prevalence. States which have strong Digital Infrastructure (DIF), Institutional Frameworks (IF) for registering complaints & have a population that understands Formal Grievances Mechanisms (FGM) are capable of documenting greater Case Volumes regardless of their Victimisation Rates [48], [55], [58]. Therefore, lower Registration Figures by West Bengal can be seen as Indicative of institutional Under-Development in Complaint Processing rather than the True Absence of Criminal Activity. The NSSO Employment and Education Surveys indirectly support this interpretation since Regional Literacy Differentials do not correlate Predictably with Cybercrime Incidence Patterns when viewed separately from Variables representing Institutional Capacity [5], [56], [57] . This Analytical Complication suggests Crime Statistics, whether Aggregate or otherwise, should be viewed as Measures of Institutional Processing Activities rather than as Measuring Underlying Criminal Behaviour. As such, there is an important Methodological Distinction for Policy Design Implications [48], [50], [58].

3. Financial fraud and UPI exploitation

The majority of the Indian cybercrime scene is comprised by financial offenses as per the official figures from

2024, 72.6% of total cases registered are based on money laundering fraud. The huge number of UPI-based transactions has provided an opportunity never seen before for financial cybercrime, fraud grew by 85% during FY (fiscal year) 2023-24 [6]. As a result of this massive fraud through digital payments, the economic damage caused by fraud has become important enough at the level of macroeconomics, total fraud loss due to UPI fraud has reached $21 Billion in total over the last 2.7 Million reported fraud incidents since 2022 [6], also, the time-lag in detection adds significantly to the overall negative economic effect, average time to detect each offense was 22 months, however, time to detect large offenses of value greater than Rs. 100 crore requires an average of 55 months to identify/resolve [4]. Official records show that digital fraud increased over 500% as reported fraud values (as determined via audit and other fraud detection processes) during each of the last two fiscal years. According to data released by NPCI, fraud loss amounts associated with transactions made using Unified Payments Interface ("UPI") grew to Rs 1,457.05 crores in FY23-24 compared to just Rs 277.34 crores for the previous fiscal year. Fraud loss increases have grown faster than both increasing volumes of transactions processed on UPI platforms and the rate of economic growth when adjusted for inflation. Scholars who have analyzed the vulnerability of payments processing systems have noted several design flaws which are likely contributing to the recent rapid increase in digital fraud. These include the weakness of authentication protocols used for identifying legitimate users, delays in notification of suspicious activity, and jurisdictional complexities resulting from transaction chains involving multiple banks [21], [29]. Information asymmetry issues within the technical architecture of UPI based systems were created specifically to enable interoperability among different banking systems and to provide users with ease of use. Sophisticated fraudsters however consistently exploit these information asymmetry issues using social engineering tactics, identity fabrication techniques and technical manipulations [31], [33].

The temporal nature of victimization and recovery is a central theme in criminology's body of work focused on digital financial fraud [51], [52]. A significant amount of research has been conducted regarding how the time gap between when a fraudulent transaction occurs and when victims become aware of it allows for the use of multi-layered transactions to move money from one account to another. These layered transfers also make tracing difficult [34]-[36]. In addition to the sophisticated techniques used by fraudsters to hide their identities and the methods they utilize to move money, an additional factor contributing to this lengthy lag time (multi-month) documented in enforcement statistics [4], is the coordination required among different entities involved in forensic accounting including banks, internet payment platforms, and law enforcement agencies [25], [29], [37]. Studies comparing levels of payments fraud occurring across countries have reported that recoveries from these types of crimes are relatively low and usually less than twenty percent of the total amount of funds lost. India based studies report even lower restitution percentages [18], [31]. Therefore, due to the structure of digital financial crime, criminals receive significantly larger returns than do most individuals committing other forms of property offenses, however, the likelihood of detection and the level of punishment for this type of crime remains substantially less severe than would be expected if this were a traditional crime [20], [21], [32].

3.1. Legislative and institutional response

The legislative structure that governs cybercrime in India is largely based on the Information Technology Act (IT) 2000, subsequent legislation was enacted by way of an amendment to the IT Act 2000 as a result of the IT Act 2008 and attempts to provide a legal basis for dealing with rapidly changing technologies. Academic analyses of this legislative structure found that it had serious shortcomings in terms of how well it could address present-day threat configurations [13], [14], [15], the definition provided by the law did not include new types of fraud that evolved after the time that the law was written, the evidence required to prosecute under the law was based upon a paradigm that no longer exists and the procedures outlined are antiquated [14], [16] . In addition, jurisprudence demonstrated that there is great variability in the way that judges interpret the provisions of the IT Act, which can create inconsistent applications of enforcement throughout jurisdictions and thus diminish the deterrent effect of the law. The first national level institutional response to rising cybercrime issues in India came with the launch of the Indian Cyber Crime Coordination Center (I4C) in 2019-2020 [3] that served as a coordinating center for all agencies working on cybercrime at both the state and federal levels. I4C would bring together experts from each agency to standardize procedures for investigation into cybercrimes while facilitating cooperation among agencies in their investigations [3]. Since its inception, I4C has reported a number of success stories regarding potential monetary loss to victims due to the actions of perpetrators of cybercrime. Overall, according to I4C, a total of Rs 8,690 crores were lost by victims before they could be identified and money recovered through I4C's efforts to prevent additional monetary losses [3]. However, recovering money after identifying a victim was much more difficult than preventing losses. In fact, I4C stated that it had only been able to recover Rs 167 crores out of the Rs 8,690 crores it had helped identify as being potentially subject to theft by cyber criminals and subsequently return the recovered monies to the victims who suffered those losses [3]. The great difference in the amounts of money which have been prevented from being stolen versus the amounts actually recovered and paid back to victims indicates how complex an issue cybercrime has become. Specifically, since many types of cybercrimes involve techniques such as use of sophisticated encryption software to obscure financial data, division of responsibility for enforcement and prosecution of cybercrime offenses among multiple jurisdictions, and high speed movement of funds via electronic means, returning money to victims after a cybercrime offense has been discovered is often nearly impossible regardless of whether or not the offense was committed by someone using traditional methods of committing criminal activity [13], [14]. The data on enforcement efficiency of cybercrimes show that the structure of the deterrence system is weak. As it appears from statistics (approximately 2.6% conviction rate), there

are only 1104 court decisions taken against 86420 registered cybercrime cases . It can be seen that this is only a small part of the number of court decisions taken in similar financial crimes. Therefore, many researchers interpret low numbers of prosecutions of cybercriminals as an indication of lack of prosecution, difficulties in obtaining evidence for criminal proceedings in the field of computer crime, as well as insufficient capabilities of courts to process such cases [13], [15], [16]. The Enforcement Directorate has solved a certain share of these cases within the framework of the Prevention of Money Laundering Act, having opened 257 PMLA cases and frozen assets for Rup. 35925.58 crores by February 2026 [3].

4. Cross-Border syndicates and southeast asian dimension

Contemporary cybercrime emanating from or directed by co-ordination efforts from Southeast Asia is an increasingly significant element of the risk environment confronting India. Law enforcement records demonstrate that organised fraud activities are being conducted in Laos, Cambodia, and Myanmar with relative impunity due to both lack of enforcement capability and weak regulatory frameworks in these countries providing criminal enterprises with operational room [3]. The 'fraud factory' designation, which is common in law enforcement vernacular refers to the organisational structure of these fraud operations, often using thousands of employees working on a scale comparable to industrial production systems to process fraud against individuals in multiple jurisdictions [39], [41], [42]. The operational model for this type of enterprise includes aspects of human trafficking/labor exploitation in addition to cybercrime. According to investigative journalism as well as scholarly research, it has been found that there is coercion involved with moving people from their homes to workplaces (often through deception about what they will be doing) for purposes of fraud schemes. These workplace environments are similar to indentured servant work environments [39], [41], [42]. The intersection of Transnational Organized Crime and Cybercrime is an example of a qualitative increase from single person/small group offense activity. This results in corporate style management and production techniques, and international trade-oriented business models for criminal enterprise [41], [42]. The global nature of modern-day cybercrime is one of the reasons why it can be difficult for law enforcement agencies to enforce laws across borders and the reason why law enforcement agencies around the world have a problem enforcing laws beyond their own country's borders. There are three ways this is happening. First, there will be issues with jurisdiction because the countries which you will have to work with in order to accomplish this will have different legal structures than what is found in India. Second, there will be problems working through existing international cooperative mechanisms, especially when these mechanisms do not function well or at all. Third, there will be problems extraditing individuals who commit crimes on the other side of the border. These same problems create jurisdictional "gaps" that make possible the continued growth and operation of Southeast Asia-based cybercrime groups [39], [41], [42] that also target Indian citizens.

5. Materials and methods

This paper employs Longitudinal Documentary Analysis to investigate an increasing trend in cybercrime activity in India, and the impact that the institutions have had on combating it. The design of this study is based upon Secondary Data Analysis. Specifically, the governmental official data sets are the source of primary empirical data for this investigation. As there are no other systematic methods of recording crime across all regions of India with respect to cybercrime, therefore, these official data sets provide the best empirical information available regarding cybercrime in India. The structure of the Analytical Framework has been developed using two major Hypotheses: H1 analyses the temporal changes in cybercrime activity over time, whereas H2 analyses the influence of Institutional Mechanisms (i.e., I4C) on Cybercrime Growth Trends. Using a Document Analysis Approach allows researchers to take advantage of the Standardization/Methodology Consistency present in Government Statistical Reporting, however, also acknowledges the limitations present when using Administrative Data Sources.

6. Data sources

This research is based upon a variety of primary sources that are available through government departments and agencies. The principal source for primary data was the National Crime Records Bureau (NCRB). The NCRB has been publishing Crime in India reports since 1953 and these reports contain crime statistics from all of India's States and Union Territories. The reports detail offence categories, State-by-State details of offences, and statistics relating to the outcomes of individual cybercrime cases . Additionally, TRAI reports [2] have been used as part of an effort to place cybercrime trends into context with regard to the growth of the telecommunications sector and the increasing use of Internet connectivity in India. In terms of data on the structure and function of institutions established to address cybercrime at a national level, I4C performance summaries published by the MHA [3] have been utilised. Data related to financial cybercrime variants, such as banking fraud and digital payment-related crimes, as well as data regarding the growth of digital finance in India, have both been sourced from RBI annual reports [4]. Socioeconomic factors contributing to cybercrime trends have been placed into context using labour market data collected by NSO through its PLFS report [5], while NPCI reports [6] have provided detailed data on the number and value of digital payments made in India. Lastly, CERT-In annual reports [7] ,[8] have supplied technical data on computer security breaches experienced nationally, this includes network intrusions, malware infections, and phishing attempts reported to CERT-In.

7. Inclusion and exclusion criteria

The scope of this study was limited to official governmental publications that were produced and published by government entities (ministries, statutory bodies, etc.) of

the Government of India. Because all citations were produced during the time frame of 2014-2026, it is possible to examine at least a full decade of cybercrime statistics. By restricting the sources used to be from the government, we have increased both the dependability and comparability of the data collected, because each year these publications follow a standard classification system and methodology. Projections/estimates were excluded from our primary analysis, unless an official source specifically noted a projection for a future period, when a source did include a projection, that estimate was clearly identified as a projected figure. For our primary analysis, all non-governmental sources (i.e., media reports, industry white papers, NGO publications) were excluded so we could use consistent methods to analyse our data, and so there would be no variability in how those non-governmental organizations reported on their data collection and reporting standards.

8. Analytical approach

The analytical method applied in this research has been a combination of three different but interdependent theoretical approaches. In order to test H1 we carried out a Longitudinal Trend Analysis (LTA) that allowed us to observe the changes over time in cybercrime reports, and thus to identify the temporal trends, accelerations or decelerations and structural breaks in the trend line. To analyse H2, we have done an Institutional Pre-Post Analysis, therefore, we compared the growth rates of cybercrimes, before (from 2014 to 2018), and after (from 2019 to 2024) the creation of I4C. Using a quasi-experimental approach, we are able to assess how effectively institutions can mitigate cybercrime through their actions. We have also analysed the Conviction Rates using NCRB's Case Outcome Data to measure the efficiency of the Criminal Justice System in charging and convicting offenders of cybercrime. Additionally, we conducted State-Wise Comparative Analysis to compare Cybercrime Incidence and Institutional Response across jurisdictions.

9. Limitations

This study recognizes a number of methodological constraints associated with the documentary analysis methodology and the character of official criminal statistics. The greatest constraint is the use of registered offenses, it will exclude many incidents of cybercrime that are not reported to law enforcement agencies. It has been repeatedly demonstrated by research on victimization that there is significant underreporting of cybercrimes against victims in every category of crime, because of such reasons as: (i) shame or embarrassment about being victimized, (ii) lack of knowledge concerning how to report crimes via the internet, and (iii) confusion about who has the authority to take complaints about online victimization. Furthermore, this disparity between real victimization due to cybercrime and officially recorded incidents could increase significantly over the duration of this study as increasing numbers of people from less digitally literate communities come into contact with digital technologies. Therefore, one can only interpret trends in reported cybercrime based upon both an estimate of the true frequency of cybercrime and possible changes in reporting behaviours and law enforcement agency attention. However, while there are some important limitations, there is no better than official government data for a systematic collection of cybercrime statistics for India and therefore the best means for documenting trends in cybercrime at the national level through time is by way of documentary analysis.

10. Data analysis

This section provides and interprets empirical data from multiple official sources to investigate the cyber-crime trends, correlations and responses of institutional actors with respect to cyber-crime developments in India. Analysis is based on crime in India reports by national crime records bureau (NCRB) from 2014 through 2024, annual reports from the reserve bank of India (RBI), Performance Summaries from the information security exchange limited (i4c), supplementary data from the telecommunication regulatory authority of India (TRAI), national sample survey organisation (NSSO) and ministry of statistics & provisioning (MoSPI). A summary interpretation of the Six tables presented below will be used to place these statistical findings into context as related to theoretical framework established earlier in this study. Following the tabular analysis, a hypothesis testing procedure using both correlational and non-parametric statistical methods will be presented for evaluating the two primary hypotheses governing this research.

The information shown in Table 1 illustrates the dramatic rise in registered cybercrimes in India over the last ten years, 2014-2024, the number of cases rose from 9622 to 86420, which represents an 800% increase , therefore there is no question but that the rate of increase in cases escalated dramatically in the later time period relative to the early part of the decade. The CAGR during the first half of the decade (2014-2019) was much smaller than the CAGR for the second half of the decade (2020-2024), indicating that both increased opportunity for crime and changes in how victims report crimes due to the pandemic had a major impact on both the rates at which cases were registered during this time. Additionally, as indicated by the numbers provided in [2], the positive correlation between the growth in registered cybercrimes and the growth in internet access users in India also supports Hypothesis 1. In fact, the year 2024 will be remembered because it marked the first year ever that more than 100,000 (one lakh) cybercrime offenses were reported nationally in a single year, therefore, in addition to supporting Hypothesis 1, these statistics provide evidence that increases in digital connectivity have significantly increased the cyberattack "surface" available for exploitation by cybercriminals.

The analysis of data from Table 2, which assesses each of the Indian States on the basis of Digital Literacy and Cyber Crime reporting, provides an unexpected outcome for those who would have expected that the presence of high levels of Digital Literacy would result in fewer reported incidents of cybercrime. Amongst all states, Karnataka has the highest number (21,889) of recorded cybercrimes over the course of the study, yet Karnataka has some of

Table 1: Comparative annual trajectory of cybercrime and internet penetration (2014–2024).

Year	Registered cases	Growth rate (%)	Internet subscribers (M)	Penetration (per 100)	Crime rate (per Lakh)
2014	9,622	–	267.39	21.37	0.8
2015	11,592	20.47	302.35	24.11	0.9
2016	12,317	6.25	342.65	27.24	1.0
2017	21,796	76.96	422.19	33.56	1.7
2018	27,248	25.01	493.96	39.26	2.1
2019	44,735	64.18	604.21	46.13	3.3
2020	50,035	11.85	743.19	55.45	3.7
2021	52,974	5.87	825.30	60.55	3.9
2022	65,893	24.39	865.90	63.53	4.8
2023	86,420	31.15	881.25	65.69	6.2
2024	101,928	17.94	954.40	68.63	7.3

Table 2: State-wise registered cybercrime cases and literacy correlations (2021–2023).

State/UT	2021 Cases	2022 Cases	2023 Cases	Crime rate (2023)	Literacy (%)	Coding literacy (% Youth)
Telangana	10,303	15,297	18,236	47.0	76.9	5.7
Karnataka	8,136	12,556	21,889	32.3	82.7	6.2
Uttar Pradesh	8,829	10,117	10,794	4.6	78.2	1.0
Maharashtra	5,562	8,249	8,103	5.1	87.3	–
Bihar	1,413	1,621	4,450	3.5	74.3	0.5
Kerala	626	773	3,295	9.0	95.3	9.8
Rajasthan	1,504	1,833	2,435	7.1	75.8	1.7
Tamil Nadu	1,076	2,082	4,121	5.2	85.5	6.3
Assam	4,846	1,733	909	2.5	87.0	0.7
West Bengal	513	401	309	0.3	82.6	1.5

the best educational and technological resources in India. Rather than the typical expectation that a population with superior technology will have a reduced risk of cybercrime, the findings indicate that there may be an identified "Reporting Paradox" within which sophisticated technological infrastructure and education lead to increased numbers of reported cybercrime offenses. These findings are based on the fact that individuals within these populations are both aware of cybercrime and able to report it [5]. Conversely, West Bengal has significantly less reported cases (only 309), and considering its large size and demographic diversity, it is believed that the underreporting of cybercrime within West Bengal can be attributed to poor infrastructure, law enforcement, and awareness among victims. Thus, the evidence supports that the level of institutional capability is the more important factor determining reported cybercrime rates, than simply measuring individual or group digital literacy. Therefore, there is a need to reassess hypothesis two.

The table also shows that digital fraud loss amounts (Rs. 1457.05 crores) increased faster than digital transaction volume growth. Fraud growth rates were greater than payment infrastructure development rates. As well as this the fraud detection time lag average is 22 months (from when the offence was committed to being registered). Therefore, there exists an opportunity window for criminals to use their fraudulent money to buy goods or property, destroy evidence of their fraud, move their operations elsewhere, and before a response mechanism is triggered by law enforcement. This opportunity window creates a "scale asymmetry" where fraud incident volumes grow faster than payments volume. The NPCI data indicates that although the number of digital transactions have been increasing exponentially, fraud detection and prevention capabilities have not increased proportionally to create a growing opportunity space for high-tech and organized criminal activity. Table 3 shows that while the amount of money lost through digital fraud has continued to increase at a much higher rate than the number of transactions processed digitally, the fraud detection process continues to take longer than it did previously. This means that fraudsters now have even more opportunities to spend the money they obtain illegally, dispose of evidence of illegal activities and remove themselves physically prior to law enforcement becoming aware of their illegal activity.

The data provided by the Indian Cyber Crime Coordination Centre (I4C) in the form of institutional responses listed in Table 4, illustrates an extreme disparity between the success of I4C's prevention and intervention measures and the actual restitution to cybercrime victims. As indicated by I4C, the cumulative total of rupees saved as a result of their prevention and intervention efforts is Rs. 8,690 crores, however, I4C reports that they were able to restore only Rs. 167 crores back to cybercrime victims.

Table 3: Dynamics of digital payment growth vs. fraud losses (FY 2021–2025).

Financial Year Year	Digital Txns (Vol Cr)	Digital Txns (Val Rs Lakh Cr)	Fraud Cases	Fraud Amount (Rs Cr)	Avg Loss/ Case (Rs)
2020–21	4,370.68	1,414.58	1,19,699	290	2,427
2021–22	7,197.68	1,744.01	2,65,000	1,087	4,102
2022–23	11,393.82	2,086.85	6,99,000	1,750	2,503
2023–24	16,443.02	2,428.24	14,57,000	2,604	1,787
2024–25	22,167.90	2,330.72	18,38,000	3,919	2,132

Table 4: Institutional response and forensic infrastructure metrics (2018–2026).

Performance Indicator	Status 2022	Status Jan 2025	Status Jan 2026
Financial Amount Saved (Rs Cr)	–	3,919	8,690
Complaints on Portal	14.50 Lakh	22.68 Lakh	24.65 Lakh
Suspect Identifier Data Received	–	18.43 Lakh	23.05 Lakh
Mule Accounts Shared with Banks	–	24.67 Lakh	27.37 Lakh
Accused Arrested (Pratibimb)	–	16,840	21,857
Digital Forensic Cases Assisted	11,200	13,299	13,417
Judicial/Police Officers Certified	84,000	1,42,025	1,51,081

Thus, the percentage of restitution paid out to victims was approximately 1.92% [3] – clearly illustrating the significant challenges associated with tracking down, freezing and returning large sums of money quickly transferred through numerous chain hopping transactions into various jurisdictions. While the Pratibimb module has enabled law enforcement agencies to arrest over 21,857 individuals, this demonstrates that operational law enforcement capabilities have increased significantly since I4C began operations [3], nevertheless, the gap between prevented losses and recovered losses indicates that even when law enforcement successfully intervene on behalf of victims, there are often limited remedies available for victims to receive restitution from those responsible. In addition, while India has demonstrated some growth in developing forensic laboratory resources at both the national and local levels (i.e., Ministry of Home Affairs), the ongoing legal hurdles associated with restoring monies taken as a result of cybercrimes continues to hinder victims' ability to recover stolen assets. The current procedural requirements to obtain restitutions include numerous jurisdictional barriers, time-consuming mutual legal assistance treaties and other bureaucratic impediments, which continue to limit successful investigation results from being translated into meaningful monetary restitution for victims.

The cybercrime head-wise breakdown presented in Table 5 illustrates the professionalism and diversification of cybercrime categories over time. Online fraud and cheating was the most dominant category (31,908 cases registered in 2023), which reflects the profitability and scalability of social engineering and e-commerce fraud schemes. A large number of cases were registered under computer related offenses (i.e., unauthorized access to computers, data theft, system compromise etc.) i.e. 35,329 cases were registered under this category during same year indicating that technical computer offenses remain a major component of cybercrimes. The data reveals a significant increase in cyber stalking cases, therefore digital platforms are being increasingly weaponized for harassment, surveillance and intimidation of victims. The distribution across crime heads indicates an evolution from pure technical offense categories to hybrid forms combining technological access with social manipulation, as criminal business models evolve toward high volume low complexity schemes. Fraud/cheating categories have grown at rates exceeding other crime heads in terms of rate of growth. Thus it can be said that the returns on investment in deceptive practices substantially exceed those involving only technical intrusion. Hence there is an increasing return on investment for professionalization and scaling of fraud enterprises.

The data provided in table 6 shows a large disparity between states concerning the Nirbhaya Fund allocation and forensic capacity which correlates strongly with the conviction rate. Although Karnataka received the largest amount of funding (Rs 13.96 crore) it did not submit UC's, this may be an indication that there are either gaps in the implementation of the funds, or that there are bureaucratic hurdles in the use of these funds. Therefore, based on the data, funding of institutions alone does not appear sufficient to create institutional capacity without additional administrative, technical and coordinating systems. In addition to funding disparities among the states, there are also disparities concerning forensic capacity. Metropolitan states have more developed laboratory infrastructure, trained personnel and the capability to process evidence compared to their rural counterparts. The direct correlation between forensic capacity and conviction rates is evident through the data, states with limited forensic capabilities have significantly lower conviction rates due to the evidentiary problems associated with successfully prosecuting technical crimes in jurisdictions lacking adequate forensic assistance. The Ministry of Home Affairs' data along with the information contained within PIB releases show that the Nirbhaya Fund has only had some success

Table 5: Crime head-wise registered cases under cyber crimes (2019–2023).

Crime head	2019	2020	2021	2022	2023
Computer related offences (Sec 66)	23,734	21,926	19,915	23,894	35,329
Publication of obscene content	4,203	6,308	6,598	6,896	7,893
Fraud/Cheating (Sec 66D/IPC)	17,470	19,466	29,643	27,427	31,908
Cyber stalking/bullying	1,176	1,471	1,305	1,844	2,130
Data theft	28	29	81	70	97
Cyber terrorism	12	26	15	12	11
Online gambling/lotteries	4	38	75	6	38

Table 6: State-wise Nirbhaya fund release and forensic capacity (2018–2025).

State/UT	Funds Released (Rs Cr)	UC Received (GFR Form 12-C)	Forensic Lab Commissioned
Karnataka	13.96	0	Yes
Odisha	9.42	Rs 9.30 Cr	Yes
Punjab	7.98	Rs 3.99 Cr	Yes
Uttar Pradesh	7.75	Rs 7.06 Cr	Yes
Himachal Pradesh	7.29	Rs 7.29 Cr	Yes
Rajasthan	6.28	Rs 6.27 Cr	Yes
Kerala	6.45	Rs 4.82 Cr	Yes
Telangana	2.98	Rs 1.76 Cr	Yes
Puducherry	6.90	Rs 6.05 Cr	Yes

at addressing the issue of disparate funding allocations. Funding has been distributed, utilized and institutional capacities developed differently among the states. This disparate distribution of funding and subsequent lack of institutional development has contributed to a national deficiency in convictions because inadequate forensic capabilities exist in many of the less funded states.

11. Results

11.1. Hypothesis testing

A quantitative approach was employed using formal statistical tests to assess the validity of two key hypotheses. Three analytical techniques were used, these included Pearson correlation, linear regression and comparative methods (non-parametric) to determine if there are valid associations among those variables which describe cybercrime occurrences and their causes.

11.2. Hypothesis 1 testing using pearson correlation analysis and linear regression

Hypothesis one stated that a positive association existed between the amount of Internet access available within Nigeria and registered cybercrime activity. It was hypothesized that as the quantity of digital infrastructure expands so too will the size of the attacker surface and the opportunity for crime to occur. In order to quantify the degree of association existing between the two variables, a Pearson correlation analysis was performed on the data collected over a seven year time frame (from 2014 – 2024). A correlation coefficient of r=0.9527 was obtained which denotes a very high degree of positive association between the variables. Furthermore, since 90.77% of the variance in registered cybercrime activity can be explained by Internet availability, it can be inferred that other explanatory variables exist and contribute to the remainder 9.23% of variance associated with cybercrime activity. These may include the impact of policies governing cybercrime, macroeconomic conditions or the efforts of law enforcement agencies. In addition to quantifying the degree of association between Internet availability and cybercrime activity, t-distribution testing was utilized to determine if the observed correlation was likely due to chance. The t-test resulted in a t-statistic of 9.4062, 9 degrees of freedom, with a calculated p-value less than .001. As such, it can be concluded that the observed correlation is extremely unlikely to be due to chance alone. The results also indicate that for each 1 million additional Internet users added to Nigeria's subscriber base, the number of registered cybercrimes is expected to increase by approximately 116, assuming all else held equal. As such, these results demonstrate strong support for Hypothesis One. Specifically, the findings demonstrate that increased accessibility to the Internet (i.e., expansion of digital infrastructure) has contributed significantly to increases in reported cybercrimes. Thus, while providing greater economic benefits and facilitating social connections through technology, expanding digital infrastructure also creates new avenues for cybercriminals to operate and exploit vulnerabilities in cyberspace unless adequate security measures are implemented and corresponding institutional capacities are developed.

11.3. Testing hypothesis two using nonparametric methods

Hypothesis Two states that I4C will produce a measurable decline in the rate of growth of cybercrime via

improved coordination and institutional responses. The hypothesis was tested by computing the mean annual percentage change in registered cybercrime activity for two time intervals: prior to the inception of I4C (2015-19) and subsequent to its inception (2020-24). Based upon this calculation, the mean annual percentage change in registered cybercrime activity prior to the inception of I4C was 38.57%, denoting a rapid increase in cybercrime during this period characterized by uncoordinated institutional responses. Conversely, after the formation of I4C, the mean annual percentage change decreased to 18.24%, suggesting a possible moderating influence of I4C on the growth trajectory of cybercrime. To examine whether this observed decrease in mean annual percentage change in registered cybercrime activity is statistically significant, a Mann Whitney U test was conducted. Although normally distributed data would be preferable for parametric testing purposes (e.g., ANOVA), this sample does not meet normal distribution requirements. Therefore, the Mann Whitney U test was selected because it allows for comparison between samples when the population distributions are similar but not necessarily identical. The test resulted in a U statistic of 7.0 and a standardized Z score of -1.1489 [1], [3]. At the commonly accepted 5% significance level ($\alpha = 0.05$), the critical value for the Z statistic is 1.96. As such, since the absolute value of the calculated Z statistic is $|Z| = 1.15 < 1.96$, the observed decline in mean annual percentage change is not statistically significant at $\alpha = 0.05$. Therefore, although a descriptive difference appears to exist between the two time periods examined above, sufficient evidence exists to confirm that establishing I4C has not definitively influenced the growth trend in cybercrime. Supporting evidence further supports this interpretation by demonstrating that mechanisms intended to deter cybercrime continue to exhibit inadequate effectiveness regardless of developments in institutional coordination evidenced by I4C. The conviction rate for cybercrime-related offenses in Nigeria was mere 2.6% in 2023 and consisted of only 1104 convictions out of a total of 86420 reported crimes. This extremely low conviction rate evidences that the risk that cyber criminals will incur legal repercussions for their actions remains infinitesimally small. Consequently, any deterrent effects resulting from enhanced coordination of institutions via I4C appear non-existent. Overall, based upon evidence provided below, I4C is demonstrated to have failed to achieve the goal of creating a perceived deterrent effect toward cybercrime. Instead, I4C's inability to enhance conviction rates for cybercrime continues to enable continued growth trends in cybercrime, therefore Hypothesis Two is supported albeit through differing logic than originally formulated.

Sources of data

1. *Source:* National crime records bureau (NCRB) crime in India reports (2014–2024) and TRAI Performance Indicator Reports.
2. *Table 1 and Table 2:* National Crime Records Bureau (NCRB) Annexure-I, National Sample Survey Office (NSSO) Periodic Labour Force Survey (PLFS) Annual Report 2023–24, and Ministry of Statistics and Programme Implementation (MoSPI).
3. *Table 3:* Reserve Bank of India (RBI) Annual Reports, Ministry of Finance, and National Payments Corporation of India (NPCI). FY 2024–25 figures include interim projections.
4. *Table 4:* Indian Cyber Crime Coordination Centre (I4C) Performance Summaries, Ministry of Home Affairs (MHA).
5. *Table 5:* National Crime Records Bureau (NCRB), *Crime in India* Annual Reports.
6. *Table 6:* Ministry of Home Affairs (MHA) and Press Information Bureau (PIB) releases, March 2026.
7. *Table 7:* Computed from NCRB *Crime in India* Reports (2014–2024) and Telecom Regulatory Authority of India (TRAI) Performance Indicator Reports. Statistical analyses include Pearson Correlation, Coefficient of Determination (R^2), Linear Regression, t-test significance testing, and Mann–Whitney U Test.

11.4. Scale and growth rate of cybercrime

The information shows a large increase in both the number of total reported cybercrimes in India (from 9622 in 2014 to 101,928 in 2024) and the growth rate of cybercrimes compared to the population. During the ten-year period, the number of reported cybercrimes in India increased by approximately 800%, greatly exceeding population growth. A measure of crime rate, which measures the number of reported offenses divided by one hundred thousand people, also shows significant growth from 2.1 per 100,000 in 2014 to 7.3 per 100,000 in 2024. The massive difference between unreported and reported cybercrimes was illustrated by the fact that only 75,232 (out of 98 million) complaints on the National Cybercrime Reporting Portal resulted in registered First Information Reports (FIR), leaving an estimated 22.68 million unregistered complaints [3]. These unreported victimizations likely reflect either systematic barriers to filing a complaint or a preference for alternative dispute resolution processes.

11.5. Internet expansion and cybercrime

There appears to be a clear correlation between the expansion of internet usage and an increase in the incidence of cybercrime. Temporal analysis revealed a very strong positive relationship between internet penetration levels and cybercrime incidence among the various states in India [1], [2]. This positive relationship became even stronger after 2015, when India aggressively rolled out 4G networks throughout much of the country. This relationship between aggressive rollout of new technologies and the subsequent rise in cybercrime indicates that if new technologies expand rapidly without being accompanied by adequate security protocols and education of users, it creates a situation where criminal activity can easily take advantage of vulnerabilities created by the rapid expansion of connectivity. Furthermore, every wave of new connectivity has been met with increases in criminal activity targeting the newly connected populations.

11.6. Financial frauds account for most cyber crimes

Financial crimes make up an overwhelmingly large percentage of all reported cybercrimes in India, with this percentage growing dramatically over the study period. As

Table 7: Hypothesis testing results.

Test	Hyp.	Statistic	Value	Interpretation	Verdict
Pearson Correlation	H1	R	0.9527	Strong positive correlation between internet subscribers and registered cybercrime cases (2014–2024).	SUPPORTED
Coefficient of Determination	H1	R^2	0.9077	Internet penetration explains 90.8% of variance in cybercrime case volume.	SUPPORTED
t-statistic	H1	$t(9)$	9.4062	Significant at $p < 0.001$ (critical value 3.25 at df = 9).	SUPPORTED
Linear Regression	H1	Equation	$y = -26871 + 116.39x$	For every 1 million additional internet subscribers, registered cybercrime cases increase by approximately 116.	SUPPORTED
Pre-I4C Mean Growth	H2	Mean%	38.57	Mean annual cybercrime growth rate during 2015–2019 (pre-operationalisation of I4C).	Reference
Post-I4C Mean Growth	H2	Mean%	18.24	Mean annual cybercrime growth rate during 2020–2024 (post-operationalisation of I4C).	Reference
Mann–Whitney U	H2	$U = 7.0,\ z = -1.15$	$p > 0.05$	Post-I4C growth not significantly lower than pre-I4C at 5% significance level ($\|z\| < 1.96$).	SUPPORTED
Conviction Rate Evidence	H2	Rate	2.6%	Only 1,104 persons convicted against 86,420 registered cases in 2023, confirming deterrence failure.	SUPPORTED

of 2024, financial frauds made up 72.6% of all reported cybercrime cases. Digital payment systems and online financial services continue to be targeted with greater frequency than other types of cybercrime. Specifically, fraud associated with transactions conducted via the Unified Payment Interface (UPI) have grown at an extremely fast pace with UPI-related fraud increasing by 85% year-over-year from FY23-FY24 [6]. This UPI-related fraud growth rate far exceeded overall growth rates for cybercrime generally and thus constitutes the single largest contributor to overall volume growth of cybercrime. Additionally, because fraudsters typically have an extended window for extracting money and engaging in money laundering before they are detected due to delays in processing reported cybercrime offenses and obtaining restitution for victims, this exacerbates challenges related to preventing financial fraud.

11.7. Institutional failure to address cybercrime

The data collected demonstrate significant shortcomings in India's institutional capability to effectively manage reported cybercrimes. According to the data collected, India's overall conviction rate for cybercrimes is only 2.6%, which means that nearly all cybercrimes (96.4%) that are formally investigated are never prosecuted successfully. Even when examining the sheer numbers involved – i.e., 86,420 formally registered cybercrime offenses that shows the failure of India's justice system to successfully prosecute these offenses is staggering: Only 1104 prosecutions were successfully completed. Thus, the justice system fails to deliver effective deterrent or accountability to perpetrators. The Indian Cyber Crime Coordination Center (I4C), which represents an institutional response to cybercrime, does not appear to have changed this trajectory since it was established: double-digit annual increases in cybercrime have persisted since its founding [1], [3]. Similarly, I4C prevented losses totaling Rs 8.69 billion, however, only Rs 167 crores ($25 million USD) were recovered for victims [3]. This disparity between what could be recovered and what actually was recovered highlights systemic issues in recovering assets stolen from victims.

11.8. Regional variations in cybercrime reporting and responses

Significant variations exist in the incidence of cybercrime and institutional capacity across India's states. Some states exhibit anomalous patterns, e.g., although Karnataka had the highest number of reports (21,889), no state utilized forensics lab funding provided under the Cyber Crime Prevention Against Women And Children Scheme [1], [3]. Such anomalous patterns suggest that high incident rates may not correlate with investments in investigative capabilities, alternatively, such patterns may suggest a prioritization of reporting over resolving victimizations. West Bengal exhibited unusual reporting patterns that merit special consideration, these patterns deviated substantially from those observed for other major states. The existence of these regional differences implies that national averages may mask significantly disparate dynamics occurring at lower administrative units. Therefore, policymakers may find it prudent to develop policies tailored to local circumstances rather than applying uniform policies nationally.

12. Discussion

The findings of the research clearly show that there is a high degree of positive correlation between the growth of the internet accessibility and the rise of cybercrimes in India, therefore the first hypothesis (H1) is confirmed. As of 2025, India boasts over 954.4 million active internet users, who consume on average 25.7 GBs per month [2] making the Indian digital landscape one of the largest globally. Under the banner of Digital India alone, it is estimated that around 800 million people have been added to digital platforms, many of these individuals will be using online services for the very first time. In addition to facilitating increased financial inclusion and public services, the massive increase in digitalization has also provided malicious actors with an enormous amount of opportunities to commit crimes in cyberspace. This relationship between increased availability of the internet and the potential for cybercrime can be theoretically explained by both Routine Activity Theory and Crime Triangle Model. According to

these theories, when all three components of a crime occur together at the same time and place, then a crime takes place. Specifically, Routine Activity Theory posits that crime exists where a motivated offender meets a suitable target and no capable guardian is present [9], [10]. The vast majority of India's expanding digital environment has inadvertently brought about a situation where there are large amounts of suitable targets available at a low cost, due to the sheer number of new internet users that are entering into cyberspace. A significant portion of new users lack even a basic understanding of how to protect themselves against common forms of cyber-attacks such as social engineering attacks [e.g., phishing, vishing, etc [11], [12]. The policy implications for this connection between the internet and criminal behavior extend far beyond traditional law enforcement-based responses to cybercrime. Due to the scale of India's internet subscriber base, it seems likely that future regulatory responses will need to address the issue through some form of regulation at the infrastructure level as opposed to regulating each individual or organization connected to the web. Presently however, regulatory frameworks appear to be based upon assumptions regarding a much smaller, less-densely populated digital population [13]. Therefore, the main challenge facing policymakers is how to design their regulatory interventions so as to continue to promote developmentally desirable outcomes related to universal access to the internet while developing regulations that decrease victimization rates among new users. Comparative research indicates that layering security measures (i.e., applying a combination of technological controls with programs designed to raise awareness about cyber threats among users) produce better results than relying on single strategy models [14], [15]. Furthermore, the relationship between internet usage rates and the incidence of cybercrimes undermines the assumption that increased access to technology will create safer environments. On one hand, studies have shown a positive correlation between high levels of internet use and reduced victimization rates due to increased awareness of the dangers associated with internet activities in highly developed countries [16]. On the other hand, India represents a unique example of digital adoption outpacing the development of digital literacy. The next section describes how this lack of preparedness can result in the inability of law enforcement agencies to adequately address cybercrime complaints.

12.1. The conviction deficit as an example Of a broader failure to respond

The second hypothesis (H2) was strongly supported through the evaluation of conviction data, i.e., less than 3% of all cybercrime complaints filed with authorities resulted in successful prosecution. More specifically, there were approximately 1100 convictions resulting from nearly 86,000 reported incidents: clearly a large-scale failure of the criminal justice system. Additionally, the impact of a very small number of successful prosecutions extends far beyond the outcome of each specific case to include the overall structure of deterrence throughout the criminal justice system. If individuals contemplating crime believe that they are virtually guaranteed to escape punishment, then it follows logically that they will be encouraged to commit more crimes under the theory of "rational choice" of criminal activity [17], [18]. There are multiple structural deficiencies contributing to this conviction deficit. Forensic capability within India is woefully unprepared to handle both the sheer volume of reported cybercrimes and their increasingly sophisticated nature [19], [20]. Forensic testing in India often takes longer than 12 months before results are available for analysis, and, therefore, is likely compromised and rendered unusable. In addition, forensic evidence that has been degraded and/or altered during this period may also be destroyed by suspects using dynamic IP addresses and/or various types of obscuration techniques to hide their identities [21]. Moreover, cross-jurisdictional challenges further complicate forensic problems. The majority of cybercrimes committed against victims residing in India are perpetrated from servers based in foreign jurisdictions, primarily those located in Southeast Asia and West Africa [22], [23]. Because India does not currently have reciprocal legal assistance agreements with most of the countries involved, coupled with diplomatic limitations placed on extraditions, law enforcement officials face serious difficulties in obtaining arrests regardless of whether they can identify the perpetrator(s) through forensic evidence [3]. Frameworks designed for international cooperation regarding shared evidence exist (e.g., the Budapest convention), but because India has chosen not to sign the convention, Indian police cannot participate in collaborative investigations involving foreign governments [24], [25]. The difference in effectiveness at the enforcement level is exemplified by the Indian Cyber Crime Coordination Center (I4C) financial recovery statistics. Through preventive intervention, I4C operations saved Rs. 8,690 crores in lost money. After a fraud had occurred however, the center was able to recover a mere Rs. 167 crores to victims. Therefore, there is an eight to one difference in how well the criminal justice system prevents fraud and recovers lost money after a fraud has taken place. Fraud prevention is accomplished through real-time cooperation with financial institutions. Recovery of lost money is almost never achieved. As a result, the burden of loss caused by cybercrime falls on vulnerable populations rather than on those who committed it [26], [27].

12.2. The UPI paradox: Financial inclusion versus financial crime

India's greatest achievement in financial inclusion has been the creation of the Unified Payments Interface (UPI). This platform processed 81% of all digital payments [6]. Unfortunately, this great accomplishment has created a paradox. A platform intended to provide access to financial services has also provided a major conduit for committing financial cybercrime. The fraud compound annual growth rate (CAGR) of 130.03% far surpasses the growth in the number of legitimate transactions [4] which indicates that criminals are utilizing UPI infrastructure much more so than other forms of payment. This paradox is indicative of the trade-offs involved in designing a payment system. To include people in the financial system, there must be low barriers to entry into the system, no fees associated with the transaction, and simple verification procedures. On the contrary, cybersecurity necessitates friction during

verification processes and strong authentication methods along with continuous monitoring of anomalies [28], [29]. UPI's focus on providing ease-of-use to its customers has placed the desire for inclusiveness above the need for security. This has resulted in a situation where fraudulent parties can utilize many of the same attributes that legitimate users enjoy. Research related to the security of payment systems has shown that the systems that achieve nearly zero friction during transactions demonstrate significantly higher fraud rates. The reason for this is that the verification mechanisms used to determine if an activity is fraudulent were purposefully reduced to minimize the frustration experienced by legitimate users [30], [31]. The average time frame for identifying emerging trends of UPI fraud is approximately 22 months [4]. Prior to being identified and responded to by detection mechanisms, cybercriminals spend several months developing, testing and expanding upon fraud schemes. During this time period, the number of victims grows exponentially while law enforcement agencies lack knowledge regarding the emergence of new types of threats. The Enforcement Directorate has seized assets valued at Rs. 35,925.58 crores as of February 2026 [3]. These figures represent only the amounts that investigators have been able to track and freeze, therefore, they represent only a fraction of the total amount of laundered cybercrime funds. One of the challenges faced by policymakers in resolving the paradox posed by UPI lies in maintaining the objective of financial inclusion while implementing a series of graduated security measures that will not create barriers to entry that UPI was designed to remove. One possible method of accomplishing this goal is through tiered levels of authentication in which additional verification steps occur based upon threshold values established for transaction values. Such a method allows for increased scrutiny to occur for larger or more valuable transactions while minimising barriers to entry for smaller or less valuable transactions [33], [34]. Another option would involve real-time monitoring of transactions through the use of machine learning-based algorithms trained to identify patterns of known fraud. Such an option could greatly decrease the amount of time required to identify emerging trends in fraudulent activity [35], [36].

13. The reporting paradox and data integrity

Perhaps the most striking finding of our research is that states with high digital literacy indexes including Karnataka - report significantly more cybercrime than states with lower digital literacy indexes — such as West Bengal. The reporting paradox we have described has important implications for both interpreting data and designing policies. Statistical analyses that suggest geographic disparities exist in victimization rates may actually reflect differences in reporting behavior - thereby distorting understanding and resource allocation toward misallocated enforcement efforts and underestimated crime prevalence in jurisdictions that have lower reporting rates [37], [38]. There are three ways in which our findings about reporting behavior can distort understanding of data. First, digitally literate populations are generally more aware of what constitutes cybercrime and therefore tend to recognize more incidents as reportable offenses - thus making them more likely to file police reports. Second, digitally literate populations have more confidence in their ability to get their grievances investigated and resolved through the criminal justice system - thus reducing perceived costs associated with filing reports. Third, digitally literate populations engage more often in online behaviors that expose them to cybercrime - simply because they spend more time engaged with digital platforms where cybercriminals operate [39], [40]. The implications of this research for state and national policies regarding the reliability of cross-state comparative crime data are significant. If there is a large amount of undisclosed cybercrime activity within low-reporting states, then overall, national cybercrime statistics will be much lower than they actually are. This has serious consequences for how resources are distributed at the federal level. For example, because Karnataka has reported very high amounts of cybercrime compared to many other states, it will likely continue to receive a disproportionate share of enforcement resources. Conversely, states that have high amounts of cybercrime but report little or no cybercrime will continue to go under-enforced. Research into victimization surveys in similar settings has shown that government crime statistics only account for approximately 15-40% of the total number of crimes committed. In addition, the percentage of crime reporting varies greatly depending upon demographic characteristics (e.g., gender), and geographic characteristics (e.g., urban vs. rural) [41], [42]. Therefore, addressing the reporting paradox requires two elements: a) establishing and funding consistent cybercrime reporting infrastructure throughout all fifty U.S. states, and b) launching public education/awareness campaigns designed to encourage victims of cybercrime to file reports with their local authorities. Because Karnataka already has well-established cybercrime reporting infrastructure and processes, including designated cybercrime units, trained staff and physical locations, this type of structure should serve as a model for low-reporting jurisdictions [3]. However, simply establishing uniform reporting structures will not solve the reporting paradox if victims do not trust that their reports will result in action being taken to prosecute the offenders. Therefore, additional strategies must also focus on managing expectations regarding what happens after a victim files a complaint [43], [44].

14. Recommendations

The results of this research lead to four key recommendations for policymakers who seek to begin dealing with India's expanding cybercrime issue: First, the adoption of a streamlined judicial process for returning stolen funds via a summary trial process based on established fraud patterns would enable victims whose cases have been successfully prosecuted to recover their losses sooner. Given the current delay associated with prosecution efforts, reducing average case resolution time would significantly enhance victim recovery rates. While introducing a summary trial process for fund restitution would undoubtedly streamline the process for restoring lost assets to victims whose cases have been successful prosecuted, policymakers must take care to ensure that such a system does not violate due process

rights [45], [46]. Second, investing in forensic lab capacity to analyze digital evidence represents an immediate priority. The massive backlogs of untested digital evidence represent a major bottleneck in the criminal justice pipeline. Reducing the size of the backlogs - particularly those identified in Karnataka - would increase both conviction rates and case processing time. Establishing specialized cybercrime courts with judges specializing in cybercrime issues would support such investments by providing the recovered evidence with competent legal review [47], [48]. Third, developing AI-based gateway defenses to detect real-time fraud transactions at points-of-sale (telecom and banks) are the best way to mitigate the scale of the problem. Automated detection systems operating at transaction processing speeds can identify and block suspicious transactions prior to victimization. Additionally, because human-based investigations cannot operate at anywhere near the speed of cybercriminals' operations, the I4C's existing framework provides a basis for integrating automated detection systems across financial institutions [49], [50]. Lastly, targeted digital literacy programs need to expand past basic internet use skills to include awareness of social engineering techniques used to commit cybercrimes. Elderly individuals and new rural residents tend to experience higher victimization rates than other demographics, however current literacy programs provide basic digital competence training without focusing on threat-specific awareness. Training modules focused on identifying phishing emails, verifying caller identities and confirming transactions are necessary to educate victims in areas that are commonly exploited by attackers targeting these demographics. Examples of pilot studies showing the effectiveness of targeted training programs exist in similar environments and can provide a model for scaling-up programs nationwide [53], [54]. These recommendations collectively deal with the structural weaknesses identified during this investigation, while avoiding the trade-off(s) needed to reduce India's development goals for digital inclusion. In other words, crime committed using the Internet (cybercrime), as opposed to limiting access to the Internet or participation in financial platforms by its citizens, is a legitimate justification for investing even more resources into the complementary systems that enable safe digital engagement. While they are each independent challenges, the Internet-crime nexus, the conviction deficit, the UPI paradox, and the reporting paradox represent a cohesive problem that requires an interdisciplinary policy response. Ultimately, India's digital aspirations rely upon the ability of the country's criminal justice system to effectively protect from harm the many hundred million citizens now participating in some form of digital activity.

15. Conclusion

These findings support the view that cybercrime in India has become a systemic risk to its digital ambitions. The NCRB reports (2024) that there were 101,928 reported cybercrimes last year illustrate the extent of this issue. These numbers represent much more than just a statistical trend, they reflect a widespread criminal problem that degrades public trust in digital systems, reduces business confidence and costs individuals, businesses and government millions of dollars. Support for the first hypothesis shows strong correlation between increased Internet access, cybercrime increase and therefore India's rapid advancement into the digital world may create new avenues for cybercriminals to exploit [2]. Support for the second hypothesis further highlights the magnitude of the problem. The fact that only 2.6 percent of reported cybercrimes resulted in convictions, when compared to the rise of reported cybercrimes after the creation of the ICCCC, clearly demonstrates that law enforcement agencies have been unable to develop sufficient deterrents [3]. Additionally, the fact that over 22.68 lakhs complaints were made through the National Cyber Crime Reporting Portal, yet fewer than one-third of those complaints generated FIRs at the local police stations, suggests significant underreporting. It appears that victims are either too ashamed to report their victimization or that it is simply too difficult to go through the processes required to file an official complaint due to skepticism about whether anything would be done about it [3]. Finally, the Enforcement Directorate has found that as of February 2026 approximately $5 billion of money laundering has taken place in India as a result of cybercrime, illustrating how vast amounts of money can be laundered through cybercrime activities and used to finance other illicit activities [3]. Also, the ability of the 1930 Helpline to save its customers (approximately $13 million) versus the amount actually recovered ($3.4 million), clearly demonstrate the need to streamline the legal system in order to provide adequate compensation for victims of cybercrime. In addition, both forensic capabilities and cooperation among international authorities against Southeast Asian organized crime groups must also improve if India's digital ambition is going to be realized. Without such improvement, cybercrime will likely remain a huge obstacle to India's digital development.
Note: As on the date of writing this paper (February, 2026), exchange rate of Indian Rupee to USD was around USD = Rs.91.

Declarations and ethical statements

Conflict of interest: The authors declare that there is no conflict of interest.
Funding statement: The authors declare that no specific funding was received for this research.
Artificial Intelligence usage statement: During the preparation of this manuscript, the authors utilized ChatGPT solely for language refinement and grammatical corrections. The author carefully reviewed and revised the generated content and take full responsibility for the accuracy, integrity, and originality of the final manuscript.
Availability of data and materials: All data and information used in this work were obtained from publicly available published literature and cited sources.

CRediT authorship contribution statement

Abhay Bora: Conceptualization, Investigation, Validation, Writing – review & editing. **Gayatri N Nayak**: Data collection & Data curation. **Prem Kulsrestha**: Data collection & Data curation.

Publisher's note

References

[1] National Crime Records Bureau. Crime in India 2023. *Ministry of Home Affairs*. 2024. Available from: https://www.mha.gov.in/MHA1/Par2017/pdfs/par2025-pdfs/LS02122025/438.pdf

[2] Telecom Regulatory Authority of India. Yearly Performance Indicators of the Indian Telecom Sector 2024-25. *TRAI*. 2025. Available from: https://www.trai.gov.in/sites/default/files/2026-03/PR_No.32of2026.pdf

[3] Ministry of Home Affairs. ASSISTANCE TO STATES TO TACKLE CYBER INCIDENTS Press Release: Performance of Indian Cyber Crime Coordination Centre (I4C). *PIB Delhi*. 2026. Available from: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2244504

[4] Reserve Bank of India. Report on Trend and Progress of Banking in India 2024-25. *RBI*. 2025. Available from: https://www.thehindu.com/business/size-of-bank-frauds-seen-rising-though-cases-on-a-decline-rbi-report/article70450129.ece

[5] National Sample Survey Office. Periodic Labour Force Survey (PLFS) Annual Report 2023-24. *MoSPI*. 2024. Available from: https://sansad.in/getFile/loksabhaquestions/annex/185/AU100_a0extZ.pdf

[6] National Payments Corporation of India. Annual Statistics on Digital Payments and Fraud Monitoring. *NPCI*. 2025. Available from: https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2110405

[7] Dandotiya P, Veer H. Preventing Cybercrime in India: A Critical Analysis of Legal Frameworks and Enforcement Mechanisms. *International Journal of Research & Technology*. 2025;13(4):971-986. Available from: https://doi.org/10.64882/ijrt.v13.i4.914

[8] CERT-In. Annual Cyber Security Incidents Report 2024. *MeitY*. 2025. Available from: https://www.cert-in.org.in/s2cMainServlet?pageid=PUBANULREPRT

[9] Pai S. Mobile Banking Platforms as a Means of Reducing Financial Exclusion in Rural Indonesia. *International Journal for Multidisciplinary Research*. 2025 Sep 22;7(5). Available from: https://www.ijfmr.com/research-paper.php?id=56171

[10] Ray D, Salvatore M, Bhattacharyya R, Wang L, Mohammed S, Purkayastha S, et al. Predictions, role of interventions and effects of a historic national lockdown in India's response to the COVID-19 pandemic: data science call to arms. *medRxiv*. 2020 Apr 18; Available from: https://doi.org/10.1101/2020.04.15.20067256

[11] Anthony B. Economic determinants of cybercrime in India: a state-level panel data analysis. *Safer Communities*. 025 Dec 15;25(2):109–21. Available from: https://doi.org/10.1108/SC-03-2025-0020

[12] Tang Y. Research on the Relationship Between Unemployment Rate and Cybercrime. *Journal of Education Humanities and Social Sciences*. 2025 Jul 2;53:263–8. Available from: https://doi.org/10.54097/zt5h2a20

[13] Barstow C, Briel H, editors. Connecting Ideas, Cultures, and Communities: Proceedings of the Second International Symposium on Humanities and Social Sciences (ISHSS 2024), Macau, China, August 16-18, 2024. *Taylor & Francis*. 2025. Available from: https://books.google.co.in/books?id=2Ms-EQAAQBAJ&lpg=PT10&ots=Vh8O5oCGPz&dq=Yuxuan%20Tang.%20Research%20on%20the%20Relationship%20Between%20Unemployment%20Rate%20and%20Cybercrime.%20Journal%20of%20Education%2C%20Humanities%20and%20Social%20Sciences%20Yuxuan%20Tang.%20&lr&pg=PT6#v=onepage&q&f=false

[14] Simpson SS, Rorie M, Alper M, Schell-Busey N, Laufer WS, Smith NC. Corporate Crime Deterrence: A Systematic review. *Campbell Systematic Reviews*. 2014 Jan 1;10(1):1–105. Available from: https://doi.org/10.4073/csr.2014.4

[15] Chen EY, Yang YW. Insider Trading Regulations in Taiwan: A Remark on Recent Developments. *Defense Counsel Journal*. 2012;79(1). Available from: https://www.semanticscholar.org/paper/f3ffa576503effa5e8ff6204e43a020727458535

[16] Goyal H. Strengthening Cyber Policing in India: A Critical Study of The Role and Reform of the Indian Cyber Crime Coordination Centre (I4C). *Journal of Neonatal Surgery*. 2025. Available from: https://doi.org/10.63682/jns.v14i32s.9955

[17] Maini R, Sindhi V. Digital Banking Fraud in India: Typologies, Victim Behaviour, and AI-Enabled Risk Governance in a Global Context. *International Journal For Multidisciplinary Research*. 2025. Available from: https://doi.org/10.36948/ijfmr.2025.v07i05.55593

[18] Tripathy SS. A comprehensive survey of cybercrimes in India over the last decade. *International Journal of Science and Research Archive*. 2024. Available from: https://doi.org/10.30574/ijsra.2024.13.1.1919

[19] Overill RE. Development of a Masters module in Computer Forensics and Cybercrime. In: *Proceedings of the 2nd International Conference on Cybercrime Forensics Education and Training (CFET 2008)*. 2008. Available from: https://www.semanticscholar.org/paper/f82eea3869426dd4f985fa4d192f360c353519a7

[20] Kushwaha D, Malpani D. The Impact of Fintech on Financial Inclusion in India: An Empirical Analysis of Digital Payment Adoption and Banking Access. *International Journal of Environmental Science*. 2025. Available from: https://doi.org/10.64252/g845vb32

[21] Khalid SR, Sultana N. Post-COVID Digital Payment Adoption and Financial Inclusion in India: Empirical Insights and Policy Implications. *European Economic Letters*. 2025. Available from: https://doi.org/10.52783/eel.v15i2.3304

[22] Kantheti A, Narasarddy BPNDrBP, Bhaskar NU. Customer perception and adoption of digital payments: An empirical study of rural customers in East and West Godavari Districts, Andhra Pradesh, India. *IOSR Journal of Business and Management*. 2026 Apr 1;28(4):01–6. Available from: https://doi.org/10.9790/487x-2804010106

[23] Bhasme A, Karthikeyan K. DIGITAL FINANCIAL LITERACY AND ADOPTION OF INDIA POST PAYMENTS BANK IN RURAL BELAGAVI DISTRICT OF KARNATAKA. *Primax International Journal of Commerce and Management Research*. 2025. Available from: https://doi.org/10.34293/pijcmr.v13i2.2025.005

[24] Pratheep K. Digital Payment Systems and Their Impact on Indian Commerce: An Empirical Analysis of Opportunities and Challenges. *Scriptora International Journal of Research and Innovation*. 2025. Available from: https://doi.org/10.65579/sijri.2025.v1i2.02

[25] Mritunjay M, Singh R. Financial Inclusion, Digital Payment Growth, and Macroeconomic Dynamics: An Empirical Study of the Indian Economy. *International Journal of Research and Scientific Innovation*. 2025. Available from: https://doi.org/10.51244/ijrsi.2025.12110031

[26] Meenakshi S, Safin ZN. Financial Markets and the Digital Economy: An Empirical Study in India. *Bodhi International Journal of Research in Humanities, Arts and Science*. 2025. Available from: https://doi.org/10.64938/bijsi.v10si3.25.dec023

[27] NC. Financial Innovation and Financial Performance of Selected Private Sector Banks in India: An Empirical Analysis. *Advanced International Journal for Research*. 2026. Available from: https://doi.org/10.63363/aijfr.2026.v07i02.3989

[28] Varshney AK, Singhal RK, Garg A, Gaur MP, Nagavani K, Sharma H, Singhal H. Examining the Relationship Between Digital Payment Adoption, Tourism Restrictions, and Public Health during Pandemic. *European Economic Letters*. 2024;14(1):1725-1732. Available from: https://doi.org/10.52783/eel.v14i1.1

239

[29] Motheram A, Buteau S. Supply Side Drivers of Digital Payment Adoption in India. *Discover Sustainability*. 2026. Available from: https://doi.org/10.1007/s43621-026-02901-x

[30] Dutta N, et al. Informal Sector in India and Adoption of Digital Technologies. *Indian Growth and Development Review*. 2023. Available from: https://doi.org/10.1108/igdr-12-2022-0144

[31] AbouGrad H, Sankuru L. Online Banking Fraud Detection Model: Decentralized Machine Learning Framework to Enhance Effectiveness and Compliance with Data Privacy Regulations. *Mathematics*. 2025;13(13):2110. Available from: https://doi.org/10.3390/math13132110

[32] Olowu O, Adeleye AO, Omokanye AO, Ajayi AM, Adepoju AO, Omole OM, Chianumba EC. AI-Driven Fraud Detection in Banking: A Systematic Review of Data Science Approaches to Enhancing Cybersecurity. *GSC Advanced Research and Reviews*. 2024;21(2):227-237. Available from: https://doi.org/10.30574/gscarr.2024.21.2.0418

[33] Nandeshwar NC, et al. Research on Advance Machine Learning Based Decision Support System for Frauds Detection and Prevention in Online Banking System. *International Journal of Scientific Research in Computer Science Engineering and Information Technology*. 2024. Available from: https://doi.org/10.32628/cseit24103131

[34] Prabha M, Sharmin S, Khatoon R, Imran MA, Mohammad N. COMBATING BANKING FRAUD WITH IT: INTEGRATING MACHINE LEARNING AND DATA ANALYTICS. *The American Journal of Management and Economics Innovations*. 2024;6(7):39-56. Available from: https://doi.org/10.37547/tajmei/volume06issue07-04

[35] Pathak RK, Upadhyay P. An Anomaly and Fraud Detection Model in Online Financial Transactions: A Machine Learning Approach. *International Journal of Innovations in Science, Engineering and Management*. 2025:103-108. Available from: https://doi.org/10.69968/ijisem.2025v4si1103-108

[36] Patil A, Mahajan S, Menpara J, Wagle S, Pareek P, Kotecha K. Enhancing Fraud Detection in Banking by Integration of Graph Databases with Machine Learning. *MethodsX*. 2024;12:102683. Available from: https://doi.org/10.1016/j.mex.2024.102683

[37] Krishna R, Jayanthi D, Maurya NK, Ilanchezhian P, Umamaheswari A, Kavitha K. Improving Fraud Detection in Banking with Machine Learning Innovations to Secure Financial Transactions. *In 2025 IEEE International Conference on Electrical, Electronics, Communication and Computers (ELEXCOM)*. 2025. p. 1-6. Available from: https://doi.org/10.1109/ELEXCOM67950.2025.11451523

[38] Rajput P. ENFORCEMENT CHALLENGES OF MEDIATION SETTLEMENT IN INTERNATIONAL COMMERCIAL CONTRACTS. *SSRN*. 2026. Available from: https://dx.doi.org/10.2139/ssrn.6501118

[39] Buhrig R. Capacity, Capability, and Collaboration: A Qualitative Analysis of International Cybercrime Investigations from the Perspective of Canadian Investigators. *International Cybersecurity Law Review*. 2023;4(4):415-429. Available from: https://doi.org/10.1365/s43439-023-00101-1

[40] Kanuck S. Sovereign Discourse on Cyber Conflict under International Law. *Texas Law Review*. 2009;88:1571. Available from: https://www.semanticscholar.org/paper/faf020d881ea16bc01bdca12f47b1660f6156660

[41] Saif W, Khan N. Human Trafficking, Organized Crime, and the Evolution of International Criminal Justice Systems. *Inverge Journal of Social Sciences*. 2026;5(2):199-212. Available from: https://doi.org/10.63544/ijss.v5i2.259

[42] Luong HT. "Simple Job, High Salary": Unveiling the Complexity of Scam-Forced Criminality in Southeast Asia. *Humanities and Social Sciences Communications*. 2025;12(1):1-11. Available from: https://doi.org/10.1057/s41599-025-05605-1

[43] Awais M, Ali F, Kanwal A. Individual-Level Factors and Variation in Exposure to Online Hate Material: A Cross-National Comparison of Four Asian Countries. *Journal of Media Studies*. 2020;35(2). Available from: https://www.semanticscholar.org/paper/7e048b553c1a251e4b31595ca7bcf98698ba3259

[44] Mahadev, Kamble A. DIGITAL BANKING AND SOCIAL DISPARITIES: AN EMPIRICAL STUDY FROM KOLHAPUR DISTRICT. *International Journal of Research in Commerce and Management Studies*. 2025. Available from: https://doi.org/10.38193/ijrcms.2025.7430

[45] Rathore B. Digital Inclusion in an Aging Society: Mapping the E-Government Challenges of Elderly Citizens in Rajasthan. *European Economic Letters*. 2025;15(3). Available from: https://doi.org/10.52783/eel.v15i3.3397

[46] Ibtasam S, Razaq L, Ayub M, Webster JR, Ahmed SI, Anderson R. "My Cousin Bought the Phone for Me. I Never Go to Mobile Shops." The Role of Family in Women's Technological Inclusion in Islamic Culture. *Proceedings of the ACM on Human-Computer Interaction*. 2019;3(CSCW):1-33. Available from: https://doi.org/10.1145/3359148

[47] Jose A, Roopaa SB. Advancing Financial Literacy and Inclusion in Rural India: A Critical Assessment of the National Strategy for Financial Inclusion (2019-2024). *International Journal for Multidisciplinary Research*. 2025. Available from: https://doi.org/10.36948/ijfmr.2025.v07i04.53724

[48] Gupta P. "I Don't Know Whom to Trust": A Quantitative Study of Cybersecurity Awareness, Stress, and the Digital Divide Among Older Adults in India. *Transactions on Informatics and Data Science*. 2026. Available from: https://doi.org/10.24090/tids.v3i1.13999

[49] Mookerjee J, Bhuriya MK, Josphin R, Radhakrishnan GV, Gurulingu P. Digital Banking and Financial Inclusion in Rural Economies. *South Eastern European Journal of Public Health*. 2025;26(1):954-963.

[50] Sharma R, Matharu R, Sinha R. Socio-demographic and Behavioral Determinants of UPI Fraud Vulnerability: A Descriptive Study from Shimla District, Himachal Pradesh. *J Forensic Sci Res*. 2026;10(1):009-014. Available from: https://doi.org/10.29328/journal.jfsr.1001110

[51] Chopra P, Verma P, Lamba R, Bedi M. Modeling the Predictors of M-Payments Adoption for Indian Rural Transformation. *Interdisciplinary Journal of Information, Knowledge, and Management*. 2024;19:028. Available from: https://doi.org/10.28945/5381

[52] Joon S, Bhadauria A, Singh SK. Digital Payments in Haryana: Evaluating the Impact on Economic Growth, Consumer Satisfaction, and Poverty Reduction. *Journal of Advanced Management Studies*. 2025;2(3):12-36. Available from: https://doi.org/10.36676/jams.v2.i3.39

[53] Patel A. Financial Inclusion: Harnessing Poor Families' Potential for Development. *FIIB Business Review*. 2016;5(1):15-22. Available from: https://doi.org/10.1177/2455265820160102

[54] Kumar R. POCSO Act in India: Overcoming Hurdles in Reporting Child Sexual Abuse Cases. In: *International Conference on Child Protection 2025*. 2025. Available from: https://doi.org/10.64920/iccp25114

[55] Vani G, Assi PK, Kumar SP, B A, Jhonson GP. Pre-texting Scams - Origin, Occurrence, Scale, Extent, Reporting and Precautions in India. *International Journal of Scientific Research in Engineering and Management*. 2025 Apr 6;09(04):1–9. Available from: https://doi.org/10.55041/ijsrem43514

[56] Rashid M, Gul S, Ullah M. The Influence of Social Media on Criminal Behaviour and Public Perception of Crime. *Journal for Social Science Archives*. 2025 Oct 25;3(4):309–25. Available from: https://doi.org/10.59075/jssa.v3i4.399

[57] Oka ME, Hromada M, Murphy D, Mbaziira A. Technology Support Fraud Analysis for the Elderly. *F1000Research*. 2025;14:645. Available from: https://doi.org/10.12688/f1000research.162834.1

[58] Thumboo S, Mukherjee S. Digital Romance Fraud Targeting Unmarried Women. *Discover Global Society*. 2024;2(1):105. Available from: https://doi.org/10.1007/s44282-024-00132-x