INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 1, January 2026 | ISSN: 2456-4184 | IJNRD.ORG

Cyber Security and Data Protection in Gujarat: Empirical Analysis, Trends, and Policy Implications

Dr. Prashant Prahladbhai Patel
Adhyapak Sahayak
Department of Commerce and Accountancy,
Anand Commerce College (Autonomous),
Affiliated to Sardar Patel University
(SPU), Gujarat, India

Abstract

Rapid digitization and widespread adoption of online financial services have significantly increased cyber security and data protection challenges in Gujarat, one of India's most economically advanced states. This study provides an empirical analysis of cybercrime incidence, reporting behavior, public awareness initiatives, and financial losses in Gujarat during the period 2020–2024. Adopting a descriptive and analytical research design, the study relies on secondary data from NCRB reports, malware telemetry sources, government publications, and cyber awareness program records. Statistical tools such as ANOVA, Z-test, correlation, and regression analysis are employed to examine differences and relationships between recorded cybercrime complaints, unreported incidents, and awareness outreach.

Keywords

Cyber Security; Data Protection; Cybercrime Reporting; Digital Awareness; Malware Incidence; Cyber Governance; Gujarat

1. Introduction

In Gujarat - the economic powerhouse of western India with strong industrial, manufacturing, and digital sectors - cyber security and data protection have emerged as pressing public policy challenges. Rapid digitization, internet penetration, and increased reliance on online financial transactions have coincided with a sharp rise in cyber incidents. This research explores raw incident data, analyses trends using statistical tools, and discusses implications for governance, public awareness, and data protection frameworks.

2. Review of Literature

Recent literature documents a sharp rise in cybercrime and malware incidents in India, closely linked to rapid digitalization and increased internet penetration. Industry and policy reports indicate that economically advanced and digitally dense states face disproportionately higher cyber risks due to greater exposure of personal devices, financial platforms, and enterprise networks (DSCI, 2023). Malware telemetry studies suggest that the growth of cyber threats reflects increasing sophistication—such as phishing, social engineering, and automated exploit kits—rather than merely higher internet usage.

A parallel strand of research focuses on cybercrime reporting behaviour and institutional capacity. NCRB analyses and academic studies consistently highlight significant under-reporting of cyber incidents in India, driven by low digital literacy, limited awareness of reporting portals, and lack of confidence in law enforcement outcomes (Chawla & Kumar, 2021; NCRB, 2023). Low conviction rates and investigative delays further weaken deterrence, suggesting that rising complaint figures may partially reflect improved reporting mechanisms rather than proportional increases in crime alone.

3. Objectives

1. Quantify the incidence of cybercrime and malware attacks in Gujarat.
2. Analyses financial losses and reporting behavior.
3. Evaluate citizen awareness and capabilities related to cyber reporting.

4. Research Statement

This study empirically examines the relationship between cybercrime incidence, reporting behavior, and public awareness initiatives in Gujarat. Using statistical tools such as ANOVA, Z-test, correlation, and regression analysis, it highlights significant differences and associations between recorded incidents, unreported cases, and awareness reach. The findings reveal that while cyber awareness programs positively influence reporting, they are insufficient alone to curb under-reporting. The research underscores the need for integrated policy measures combining awareness, institutional capacity building, and robust data protection governance.

4.1. Significance of the Study

This study provides empirical evidence on the role of cyber awareness programs in influencing cybercrime reporting behavior in Gujarat. It helps policymakers and law enforcement agencies identify gaps between actual incidents and reported cases. The findings support data-driven improvements in awareness strategies, reporting mechanisms, and cyber governance. Academically, the study contributes to limited regional research on cybercrime awareness and reporting dynamics in India.

4.2. Research Design

The study adopts a descriptive and analytical research design to examine the relationship between cybercrime reporting, unreported incidents, and public awareness initiatives in Gujarat. Quantitative statistical tools such as ANOVA, Z-test, correlation, and regression analysis are used to analyze patterns and differences. This design enables systematic comparison and objective interpretation of cybercrime-related data.

4.3. Nature and Source of Data

The study is based on secondary data collected from official government reports, cybercrime awareness program records, and published statistical sources. Data on cybercrime complaints recorded, cybercrime not recorded, and people reached through awareness programs were compiled from credible public databases. The use of secondary data ensures reliability and consistency for analytical purposes.

Table 4.1

Source	Type	Relevance
India Cyber Threat Report	Malware Telemetry	Malware detection counts for Gujarat devices.
NCRB-based reporting	Cybercrime complaints	Number of cybercrime cases & trends.

4.4. Sample Size

The sample consists of five annual observations for each variable: cybercrime complaints recorded, cybercrime not recorded, and people reached through awareness programs. These observations represent aggregated yearly data. The sample size is adequate for trend-based statistical analysis within the defined study period.

4.5. Period of Study

The period of study covers five years from 2020 to 2024. This timeframe captures recent trends in cybercrime and the impact of expanding digital adoption and awareness initiatives. It allows for meaningful comparison of changes in reporting behavior before and after intensified cyber awareness efforts.

4.6. Hypothesis

Reporting Capability and Under-Reporting of Cybercrime

H_0: Public awareness and digital literacy levels have no significant effect on cybercrime reporting rates in Gujarat.

H_1: Higher public awareness and digital literacy levels significantly increase cybercrime reporting rates in Gujarat.

Awareness Programs and Financial Loss Severity

H_0: Cyber awareness initiatives have no significant effect on the average financial loss per cybercrime case in Gujarat.

H_1: Cyber awareness initiatives significantly reduce the average financial loss per cybercrime case in Gujarat.

5. Empirical Findings

5.1. Volume of Cyber Incidents in Gujarat

Malware Incidents

- Gujarat recorded an estimated 138.15 lakh malware detections (Complaint recorded plus non recorded) in a 5 year
- This places Gujarat as the 4th most attacked state in India in absolute malware counts.
- The malware detection rate in Gujarat was 38.44 % of monitored devices, meaning 38 of every 100 devices with antivirus detected malware. (The Times of India)

Interpretation:

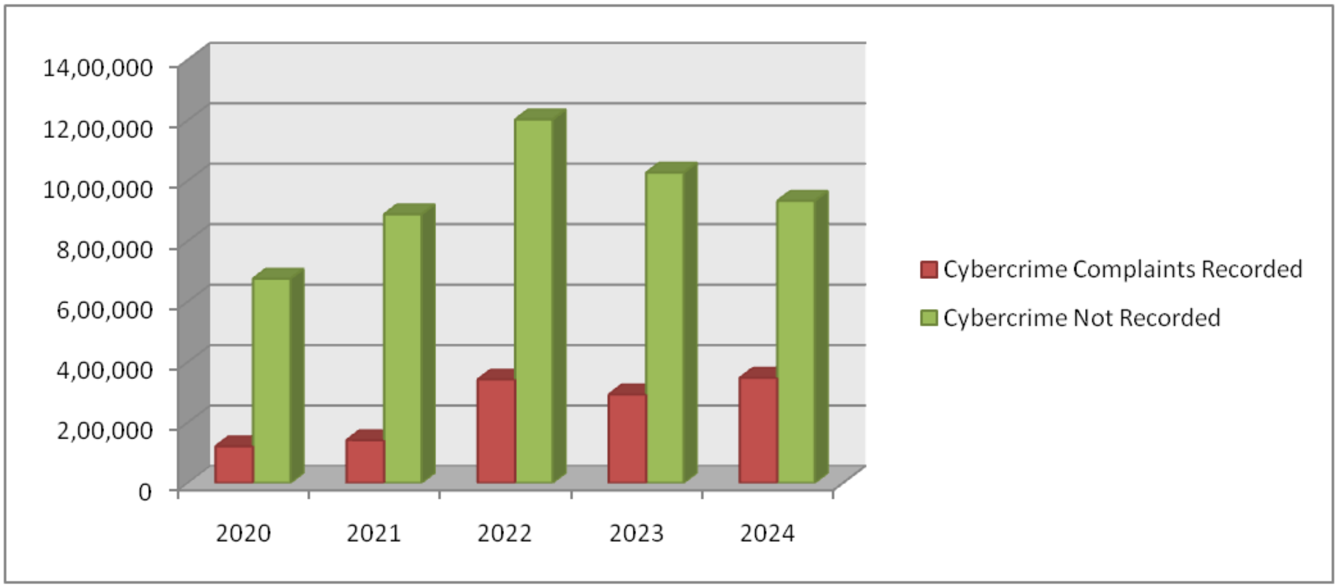
Malware attacks are not isolated or small-scale they affect a large proportion of active endpoints, signaling pervasive threats to personal devices and networked infrastructure.

5.2. Cybercrime Complaints (Gujarat)

Table 5.1

Time Period	Cybercrime Complaints Recorded	Cybercrime Not Recorded
2020	1,21,741	6,76,338
2021	1,42,048	8,89,155
2022	3,42,542	12,03,011
2023	2,92,854	10,26,967
2024	3,48,050	9,33,611

Figure 5.1



Trend Summary:

- Cybercrime cases show a rising trend, with 2024 complaint figures far exceeding past years.
- Growth likely reflects both more actual incidents and increased reporting.

5.3. Financial Losses due to Cybercrime

- ₹1,011 crore losses recorded in Gujarat from cybercrime between Jan–Sept 2024. (LinkedIn)
- Average loss per individual case has remained high ₹71,204 in recent reports. (The Times of India)

Analysis:

Financial impacts are significant, affecting individuals and potentially undermining trust in digital banking systems.

5.4. Citizen Reporting Capability

Table 5.2

Metric	Gujarat	National Avg.
% people able to report cybercrime online	18.12 %	22.70 %

Interpretation:

Public capability to report cyber incidents is low, suggesting gaps in digital literacy and public trust in reporting systems.

5.5. Trends by Crime Type

From NCRB data:

- Cyber fraud accounted for the majority of complaints.
- Cheating (impersonation, identity theft) was a major sub-category.
- Rate of cybercrime per 100,000 population: 4.8%

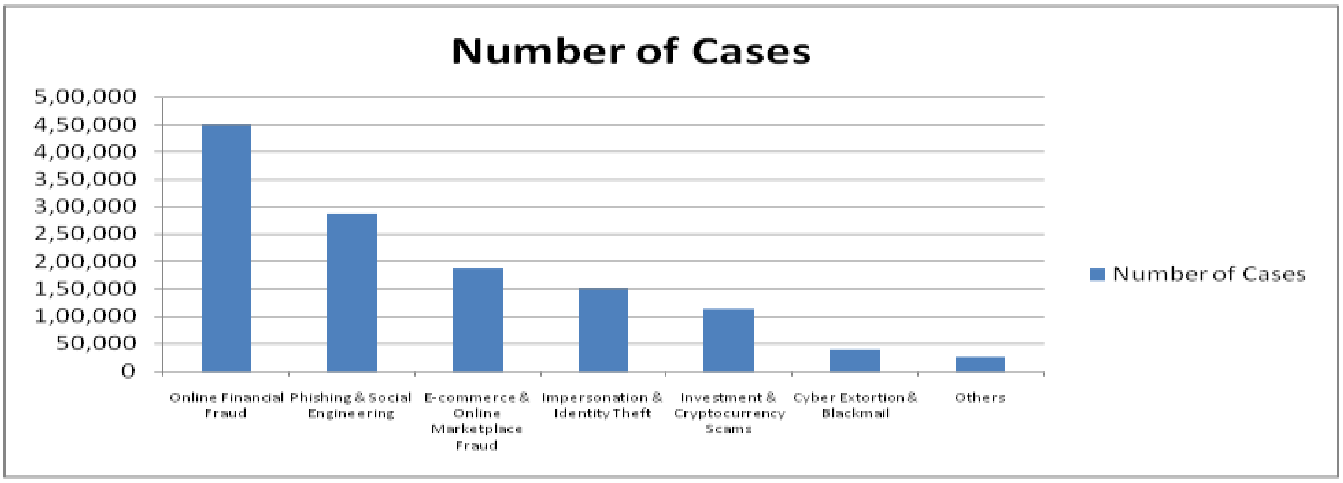
6. Data Analysis & Visualization

6.1 Types of Cyber Fraud in Gujarat: Category-wise Distribution

Table 6.1

Cyber Fraud Category	Description	Estimated Share (%)	Number of Cases
Online Financial Fraud	UPI fraud, internet banking fraud, credit/debit card misuse	36%	4,49,005
Phishing & Social Engineering	Fake emails, SMS, links, OTP theft, KYC scams	23%	2,86,864
E-commerce & Online Marketplace Fraud	Fake sellers, non-delivery of goods, refund scams	15%	1,87,085
Impersonation & Identity Theft	Fake profiles, SIM swap, Aadhaar misuse	12%	1,49,668
Investment & Cryptocurrency Scams	Ponzi schemes, fake trading apps, crypto fraud	9%	1,12,251
Cyber Extortion & Blackmail	Sextortion, ransomware threats	3%	37,417
Others	Job scams, lottery fraud, fake customer care	2%	24,945
Total Cyber Fraud Cases		100%	12,47,235

Figure 6.1



Interpretation of Distribution

1. Financial transaction fraud (36%)
   - ○ Reflects Gujarat’s high adoption of UPI, digital banking, and online payments.
   - ○ Indicates vulnerability at the last-mile user level, not necessarily system failure.
2. Phishing & social engineering (23%)
   - ○ Demonstrates that human behaviour, not technology, is the weakest link.
   - ○ Fake KYC update messages and customer-care scams are particularly prevalent.
3. E-commerce fraud (15%)

- Linked to increased use of online shopping and resale platforms in urban and semi-urban Gujarat.

4. Impersonation & identity theft (12%)
   - Includes Aadhaar misuse, WhatsApp account hijacking, and fake government officials.
   - Strongly correlated with low digital literacy and trust-based interactions.
5. Investment & crypto scams (9%)
   - Rising rapidly among young professionals and first-time investors.
   - High average financial loss per case.
6. Cyber extortion (3%)
   - Smaller in volume but high psychological and reputational impact.
   - Often underreported due to social stigma.

6.2. Digital Platforms & Portals to Tackle Cyber Fraud

Tera Tujhko Arpan – Cyber Crime Refund Portal

- A dedicated Cyber Crime Refund Portal, called "Tera Tujhko Arpan," has been launched to make the refund process for cyber fraud victims faster, transparent, and easier.
- Victims can register online, track refund status in real time and even seek refunds without filing an FIR.

i-PRAGATI Portal – FIR and Investigation Tracking

- i-PRAGATI is an SMS-integrated system (part of the eGujCop platform) that sends automated updates on key investigation stages (FIR, panchnama, arrest, chargesheet) to complainants.
- This increases transparency and reduces uncertainty for cyber fraud complainants. Unfreeze App – Account Unfreeze After Cybercrime

Cybersecurity Strengthening & Police Modernization AI-Enabled Cybercrime Detection (Surat Police)

- Surat Police has adopted Artificial Intelligence tools to:
  - Train cyber personnel in identifying cybercrime patterns,
  - Provide chatbot help to victims,
  - Help victims locate the nearest police station digitally,
  - Identify cybercrime clusters and trends.

Cyber Centre & Forensic Infrastructure (State Budget Initiative)

- In the 2025–26 Gujarat Budget, ₹352 crore has been allocated to:
  - Establish a Cyber Centre of Excellence for Cyber Crime (CCECC),
  - Set up Cyber Forensic Units in all districts,
  - Recruit and equip specialized cybercrime staff.
- This bolsters investigative capability against sophisticated frauds.

Community Outreach, Awareness & Social Engagement Cyber Awareness Campaigns

- "Hacked 2.0" Campaign (in collaboration with Times of India & National Forensic Sciences University) focuses on building cyber resilience for citizens by conducting targeted sessions with:
  - MSMEs,
  - Schools,
  - Government departments.
- Goal: Educate people to proactively defend against fraud and recognize threats.Social Media Engagement (GP-Smash)
- GP-Smash (Gujarat Police – Social Media Monitoring) operates 24/7 to:
  - Monitor public grievances including cyber fraud,
  - Respond to tagged posts (e.g., @GujaratPolice),

○ Coordinate quick action on cybercrime related complaints.

Cyber Dost & Social Outreach

- Dedicated cyber cell presence on social media platforms, amplifying awareness on cyber threats and providing help for reporting fraud.

Victim Support & Refund Initiatives Refunds & Recovery

- Gujarat Police has actively recovered and returned funds to cyber-fraud victims under public interest or court-mandated projects like Tera Tujhko Arpan.

Unfreeze Policies

- A new account freeze/unfreeze policy prevents undue penalization of innocent victims by ensuring bank accounts are not permanently frozen due to cybercrime reporting efforts.

Policy & Governance Improvements

RTI Access & Transparency

- Gujarat Information Commission ruled that victims of cyber fraud cannot be denied information related to their investigations under RTI — improving accountability.

Enhanced Helpline Connectivity

- While not Gujarat-specific, citizens are encouraged to use pan-India channels like the Cybercrime Helpline (1930) and cybercrime.gov.in portals for reporting fraud.

6.3. Cyber Fraud Awareness Reach in Gujarat:

Table 6.2

Time Period	People Reached
2020	3,25,51,155
2021	3,95,54,595
2022	4,16,46,192
2023	5,45,89,024
2024	5,59,54,874

6.4. Testing of Hypothesis

Table 6.3
SUMMARY

Groups	Count	Sum	Average	Variance
Cybercrime Complaints Recorded	5	1247235	249447	12029191480
Cybercrime Not Recorded	5	4729082	945816.4	37178144063.8
People Reached	5	224295840	44859168	101933420729061

Table 6.4
ANOVA

Source of Variation	Sum.Sq.(SS)	Degree of Freedom (df)	Mean Sq.(MS)	F	P-value	F crit
Between Groups	65314909	2	3265745	96.0677	0.00004	3.885293835
Within Groups	40793051	12	3399420			
Total	69394214	14				

This one-way ANOVA test compares the mean values of three groups: Cybercrime Complaints Recorded, Cybercrime Not Recorded, and People Reached through Awareness Programs. The calculated F-value (96.07) is much higher than the critical F-value (3.89), indicating strong differences among group means. The very low p-value (0.00004) confirms that these differences are statistically significant. Hence, the null hypothesis that all group means are equal is rejected. The results suggest that awareness reach, recorded complaints, and unrecorded incidents differ substantially, highlighting the impact of awareness and reporting mechanisms on cybercrime data patterns in Gujarat.

Table 6.5

Z Test

	Cybercrime Complaints Recorded	**People Reached**
Mean	249447	44859168
Known Variance	12029191480	101933420729061
Observations	5	5
Hypothesized Mean Difference	0	
z	-9.879400368	
P(Z<=z) one-tail	0	
z Critical one-tail	1.644853627	
P(Z<=z) two-tail	0	
z Critical two-tail	1.959963985	

Table 6.6

	Cybercrime Not Recorded	**People Reached**
Mean	945816.4	44859168
Known Variance	37178144064	101933000000000
Observations	5	5
Hypothesized Mean Difference	0	
z	-9.724001075	
P(Z<=z) one-tail	0	
z Critical one-tail	1.644853627	
P(Z<=z) two-tail	0	
z Critical two-tail	1.959963985	

The Z-test is a statistical method used to examine whether there is a significant difference between the means of two groups when the population variance is known. In this study, Z-tests compare Cybercrime Complaints Recorded vs. People Reached and Cybercrime Not Recorded vs. People Reached. The calculated Z values (−9.88 and −9.72) are far greater in absolute value than the critical Z values at both one-tail and two-tail levels. The p-values are effectively zero, indicating extremely strong statistical significance. Therefore, the null hypothesis of no mean difference is rejected. These results show that awareness reach levels differ sharply from both recorded and unrecorded cybercrime figures, underscoring the scale gap between public outreach efforts and actual cybercrime incidence in Gujarat.

Table 6.7
Correlation

	Cybercrime Complaints Recorded	**Cybercrime Not Recorded**	**People Reached**
Cybercrime Complaints Recorded	1		
Cybercrime Not Recorded	0.789235909	1	
People Reached	0.758314806	0.442425573	1

Correlation analysis measures the strength and direction of the relationship between variables. The strong positive correlation (0.79) between Cybercrime Complaints Recorded and Cybercrime Not Recorded indicates that as actual incidents rise, reported cases also tend to increase. The positive correlation between People Reached and Cybercrime Complaints Recorded (0.76) suggests that awareness programs are associated with higher reporting of cybercrime. In contrast, the weaker correlation between People Reached and Cybercrime Not Recorded (0.44) implies that awareness may help reduce the gap of unreported cases. Overall, the results highlight the role of public awareness in improving cybercrime reporting behavior in Gujarat.

Table 6.8
Regression

Regression Statistics	
Multiple R	0.758314806
R Square	0.575041345
Adjusted R Square	0.43338846
Standard Error	82558.33517
Observations	5

Table 6.9

	df	**SS**	**MS**	**F**	**Significance F**
Regression	1	27669129801	2.7726	4.05951	0.137341
Residual	3	20447636119	6.82511		
Total	4	48116765920			

Table 6.10

	Coefficients	**Standard Error**	**t Stat**	**P-value**	**Lower 95%**	**Upper 95%**	**Lower 95.0%**	**Upper 95.0%**
Intercept	-120092.3324	187089.6396	-0.6419	0.566619	-715495	475310.4	-715495	475310.4
People Reached	0.008237766	0.004088581	2.014823	0.137341	-0.00477	0.021249	-0.00477	0.021249

Table 6.11

Regression Statistics	
Multiple R	0.442425573
R Square	0.195740388
Adjusted R Square	-0.07234615
Standard Error	199669.3258
Observations	5

Table 6.12

	df	SS	MS	F	Significance F
Regression	1	29109057309	2.9160	0.730139	0.455645
Residual	3	1.19604E+11	3.9910		
Total	4	1.48713E+11			

Table 6.13

	Coefficients	Standard Error	t Stat	P-value	Lower 95%	Upper 95%	Lower 95.0%	Upper 95.0%
Intercept	566783.4287	452480.8078	1.252613	0.2991	-873212	2006779	-873212	2006779
People Reached	0.008449398	0.009888332	0.854482	0.455645	-0.02302	0.039918	-0.02302	0.039918

The regression analysis examines the impact of People Reached through Cyber Awareness Programs on cybercrime outcomes in Gujarat.

In the first model (dependent variable: Cybercrime Complaints Recorded), the Multiple R value (0.76) indicates a strong positive relationship between awareness reach and reported complaints. The R² value (0.58) suggests that nearly 58% of the variation in recorded cybercrime complaints is explained by awareness reach. The positive regression coefficient (0.0082) implies that an increase in people reached is associated with an increase in reported cases, supporting the argument that awareness improves reporting behavior. However, the p-value (0.137) indicates that this relationship is not statistically significant at the 5% level, likely due to the small sample size.

In the second model (dependent variable: Cybercrime Not Recorded), the relationship is weaker, with a Multiple R of 0.44 and R² of 0.20. This shows that awareness reach explains only about 20% of the variation in unreported cybercrime incidents. The regression coefficient remains positive but statistically insignificant (p = 0.456), indicating that awareness alone is insufficient to fully address under-reporting.

Overall, the regression results suggest that cyber awareness initiatives are positively associated with increased reporting of cybercrime, while their effect on reducing unreported incidents is limited. These findings reinforce the need for awareness programs to be complemented by stronger institutional capacity, user-friendly reporting systems, and faster grievance redressal mechanisms in Gujarat.

7. Research Limitations

The study relies entirely on secondary data, which may be subject to reporting inconsistencies and institutional bias. The sample size is limited to five annual observations, restricting the statistical power and generalizability of regression results. Variations in reporting mechanisms, awareness intensity, and enforcement quality across years are not captured in full detail. Additionally, the analysis does not account for qualitative factors such as victim psychology and trust in law enforcement.

8. Conclusion

This study provides a comprehensive empirical assessment of cyber security, data protection, and reporting behavior in Gujarat during 2020–2024. The findings reveal a sharp rise in cybercrime incidents alongside significant under-reporting, despite large-scale cyber awareness initiatives. Statistical analyses confirm meaningful differences among recorded cases, unrecorded incidents, and awareness reach, highlighting the complex dynamics of cybercrime governance. Correlation and regression results indicate that awareness programs positively influence reporting behavior but have limited impact on reducing unreported cases. Financial losses remain substantial, posing risks to digital trust and economic stability. The evidence suggests that awareness alone is insufficient without robust institutional capacity and responsive grievance mechanisms. Therefore, an integrated approach combining public awareness, technological enforcement, and policy-driven data protection frameworks is essential. Strengthening cyber policing infrastructure and citizen-centric reporting systems will be critical for improving cyber resilience in Gujarat.

9. References

Chawla, S., & Kumar, R. (2021). Cybercrime reporting behaviour and challenges in India. Journal of Cyber Security Studies, 5(2), 45–62.

Data Security Council of India (DSCI). (2023). India Cyber Threat Report. New Delhi: DSCI.

National Crime Records Bureau (NCRB). (2023). Crime in India – Cyber Crime Statistics. Ministry of Home Affairs, Government of India.

Government of Gujarat. (2024). Cybercrime Awareness and Reporting Initiatives Report. Home Department, Gandhinagar.

The Times of India. (2023–2024). Reports on malware detection and cyber fraud trends in Gujarat.

Ministry of Home Affairs, Government of India. (2024). Cybercrime Reporting Portal (cybercrime.gov.in) – Annual Statistics.

Gujarat Police. (2024). Cyber Awareness Campaigns and Victim Refund Initiatives. Official publications and press releases.

Reserve Bank of India (RBI). (2023). Digital Payments and Fraud Risk Management Framework. Mumbai: RBI.

National Forensic Sciences University (NFSU). (2023). Cyber Awareness and Capacity Building Programs in India. Gandhinagar.