“A statistical analysis of cyber security challenges in Gujarat’s financial system (2010-2025): Towards sustainable digital finance for Atmanirbhar Bharat and Make in India”

Rahul Rajendra Patil.
Ph.D.-Research scholar,
Veer Narmad Soth Gujarat University, Surat.
Email: rahul97257@gmail.com

Dr Mohanbhai Namdev Mane.
Assistant Professor and Head
Department of Statistics,
SIR K.P. College of Commerce Surat, Gujarat.
Email: mohanmane641971@gmail.com

Abstract:

This study investigates cyber security challenges in the financial system of Gujarat from 2010 to 2015, Integrating both primary and secondary data sorces. Using statistical methods such as Chi-squre test ANOVA, logistic regression, ARIMA forecasting and factor/cluster analyis the research assesses demographic awareness, institutional preparedness and financial losses associated with cyber frauds. Findings highlights increasing incident trends, significant demographic variations in awareness and institutional gaps in preparedness. Policy recommendations emphasize region-specific awareness programs and stronger institutional resilience frameworks. “The outcomes provide insights into strengthening Gujarat’s financial ecosystem in line with Atmanirbhar Bharat and Make in India initiatives, promoting sustainable digital finance.”

1. Introduction:

The financial services sector has undergone a dramatic transformation in the last two decades driven by Digitization, Fintech innovations and Intervention Such as the digital India programmed in Gujarat one of the Indias fastest growing states in terms of industrial and financial activities. Banking penetration and digital adoption have been expanding rapidly with the increased reliance and online banking unified payments interface UPI digital wallets and fintech platform financial transaction have become faster more accessible and more efficient.

However, this digital revolution has introduced significant cybersecurity challenges. Cyber frauds, phishing attacks, ransomware, identity theft and unauthorized fund transfer have become more frequent, targeting both institutional system and individual customers. According to RBI fraud reports (2010-2025) and CERT in annual reports, there has been a five-fold increase in cyber fraud cases in past 15 years, with a parallel rise in the magnitude of financial losses. For instance, while 12 cyber fraud cases were reported in 2010 in Gujarat, by 2025 this number had reached 144, with cumulative financial losses estimated at Rs.28.3 crores. These figures reveal not only the increasing frequency of incidents but also the rising financial impact of cybercrime.

“These challenges directly impact India’s vision of Atmanirbhar Bharat and Make in India, where secure digital finance is the backbone of economic self-reliance and industrial growth.”

The Banking, financial Services and insurance (BSFI) sector is particularly vulnerable because of its high-value data and customer volume. Although institutions such as private banks have invested heavily in IT infrastructure and cyber risk management frameworks, Public and cooperative banks in Gujarat often lag risks At the same time, customer-related

factors such as education, income level and Digital literacy also influence susceptibility to cyber threats.

From a statistical perspective, there is a need to Quantify these risks and test the relationships between demographic factors, institutional preparedness and cyber fraud incidents. Models such as Chi-Square tests can assess associations between demographics and awareness, ANOVA can compare preparedness across bank types, logistic regression can identify predictors of victimization and ARIMA time-series forecasting can predict future fraud trends. In addition, factor analysis can reveal the latent dimension of preparedness (such as policy, technology, training), and cluster analysis can classify institutions based on their risk exposure.

Despite the importance of cybersecurity in financial systems, most existing studies in India are Either national in scope or descriptive in nature, offering limited statistical depth or regional focus. Specifically, South Gujarat and Gujarat state-level analysis are scarce creating a gap in localized empirical evidence addressing this gap is crucial for tailoring policy members designing awareness programs and strengthening institutional risk management.

This research thus aims to provide a statistically rigorous, region-specific analysis of cybersecurity challenges in Gujrat's financial systems. By Combining secondary data (RBI, CERT-In, Gujarat police cybercrime cell) with primary survey data (financial customer and banking professional), study Intends to:

1. Evaluate trends in cyber frauds and financial losses over 2000-2025.
2. Examine demographic influence on awareness levels.
3. Assess preparedness across bank types.
4. Forecast future cybercrime patterns.
5. Propose data driven policy Interventions Tailored to Gujarat.

In doing So the study makes both an academic contribution (advancing the use of statistical model in cybers risk research) and a practical contribution (providing actionable insights for regulators and institutions).

2. Review of literature

2.1 Global Perspectives on Financial Cybersecurity

The International Monetary Fund (IMF,2019) emphasized that cyber security incidents are no longer isolated events but systematic risk threatening financial stability.

Similarly, the OECD (2020) provided policy recommendation on building financial sectors Resilience, focusing on institutional investment in security infrastructure, Governance and monitoring mechanisms.

Globally, Anderson et al. (2013) Highlighted how the economics of cybercrime makes financial services the most targeted sector due to high value data and the complexity of interlinked system in a European context.

Bouveret (2018) modeled Systematic cyber risk in the banking sector estimating potential losses exceeding billions in case of large-scale attacks. These works stress the need for both predictive modelling and localized risk assessments.

2.2 Cybersecurity in the Indian BFSI Sector

Indian literature largely focuses on national level trends.

Bhat and Shah (2000) examined cyber risk management strategic Indian banks finding that Most institutions adopt a reactive rather than proactive approach.

Sharma Yadav and Bansal discuss UPI related faults identifying vulnerabilities in infrastructure and customer awareness.

From a statistical perspective, Kumar and Mehta (2016) Applied logistic regression to model predictors of cyber frauds victimization, concluding that digital literacy and income level significantly affect susceptibility. .

NASSCOM-DSCI (2018) Reports also stress the need for workforce training and organizational resilience in the BFSI sector.

Doctoral-level contribution also enriches the Indian context.

Anand (2015) Analyzed India's cyber security policy frameworks, concluding that fragmented government structures weakness Resilience.

Devi (2020) Studied the challenges of Digital India program, emphasizing the gap between adoption and security mechanisms.

Dayma (2021) Provided a legal perspective on cyber fraud in banking, analyzing Institutional accountability in cyberspace.

Despite this important contribution very few studies have explicitly linked cybersecurity in the Indian financial sector with border national development programs such as Digital India, Atmanirbhar Bharat and Make in India. Positioning cybersecurity is not only a technical requirement but also a driver of economic Self-reliance and industrial growth makes this study unique as it isconnects statistical evidence from Gujarat with India's largest development vision.

2.3 local insights: Gujarat and south Gujarat

At a state level, Desai(n.d.) in M.Phill thesis at Veer narmad south Gujarat University, studied financial inclusion and highlighted digital literacy as a barrier to safe adoption of financial technology in South Gujarat.

Hasmukhbhai (2024) Explored consumer prospection towards cybercrime in Gujarat, finding that trust deficit and lack of awareness were significant the rural populations compared to urban customers.

Institutional reports from the Gujarat Police cybercrime cells confirm an annual rise in both the number of reported cyber fraud cases and financial losses between 2010 to 2025, Consistent with National RBI reports.

However no systematic statistical modeling or Inferential analysis at the Gujarat level has been conducted.

3. Research Gap

Thus, this research addresses the gap by:

1. Conducting 15 years statistical trend analysis (2010-2025) of incident and financial losses in Gujarat.
2. Testing demographic and institutional hypothesis using inferential methods.
3. Applying predictive (ARIMA) and structural (factor/cluster) models for risk profiling.
4. Proposing policy-oriented interventions tailored for Gujarat's BFSI sector.

4. Objectives

Primary Objectives

1. To analyze the trend of cyber fraud incidents and financial losses in Gujarat (2010-2025).
2. To assess the relationship between customer demographics and cybersecurity awareness.

Secondary Objectives

1. To Compare Preparedness levels across public, private and cooperative banks.
2. To develop predictive models for forecasting frauds using ARIMA.
3. To provide policy-oriented recommendations for regional financial cybersecurity resilience.
4. To align cybersecurity resilience in Gujarat's financial systems with the border national goals of Atmanirbhar Bharat and Make in India.

5. Hypotheses

1. **H_{01}:** No significant relationship exists between education level and cybersecurity awareness.
2. **H_{11}:** Education level significantly influences cybersecurity awareness.
3. **H_{02}:** There is No difference in preparedness levels between public, private and cooperative banks.
4. **H_{12}:** preparedness level significantly differs across bank types.

6. Research Methodology

6.1 Research Design

This study adopts a quantitative research design supported by descriptive and inferential statistics. The design allows for both trend analysis of cyber fraud (2010-2025) and the evaluation of awareness and preparedness levels across demographics group and financial institutions. A cross-sectional survey was used for primary data, while Secondary data was obtained from RBI CERT-In and Gujarat Police Cyber Cells Reports.

6.2 Population and Sampling

The population includes two categories:

1. **Retail financial customers in Gujarat-** individual using online banking, UPI, mobile wallets, and offer fintech platforms.
2. **Financial institutions and professionals-** including Public, Private and Cooperative banks, NBFCs and fintech firms.

A stratified random sampling technique was used to ensure adequate representation across urban, semi-urban and rural areas, within each stratum, respondents were selected randomly.

Sample Size justification:

The sample size was determined using **Cochran's Formula:**

$$n_0 = \frac{Z^2\, p(1-p)}{e^2} = \frac{(1.96)^2\, 0.05(0.05)}{0.0025} = 384.16$$

Thus, a minimum of 400 financial customers were surveyed to account for non-responses. In addition, 30 financial professionals were purposively sampled for expert interviews.

6.3 Data Sources:

- **Primary Data:**
  - Structured questionnaire administrator to relate customers (covering demographics, awareness, digital behavior and experience of fraud).
  - Semi-structured interviews with financial professionals on preparedness and policy frameworks.
- **Secondary Data:**
  - RBI reports, CERT-In logs, Gujarat Police Cyber Sales reports (2010-2025).
  - Published Research Papers, Theses and government documents.

6.4 Research Variables

- **Independent variables:** Age, Education, income, Occupation, Region, Institution Type, Digital Banking Frequency, Training Programs.

- **Dependent variables:** Cyber fraud incidents, financial loss, Awareness Score, Institutional preparedness.

6.5 Statistical Tools and Software

- **SPSS v26**- chi-square, ANOVA, Regression analysis.
- **R/Python-** ARIMA forecasting, Cluster analysis.
- **Excel**- Descriptive summaries, Tables and Charts.

6.6 Statistical models and Equations:

1. **Chi-Square Test**

$$\chi^2 = \frac{(O-E)^2}{E}$$

To test association between demographics and awareness

2. **AONOVA**

$$F = \frac{MS_{between}}{MS_{wuthin}}$$

To Compare preparedness across institutions Types.

3. **Logistic Regression**

$$log\left(\frac{p}{1-p}\right) = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_n X_n$$

To analyze the relationship between independent variables and dependent variables

4. **ARIMA**

$$Y_t = \alpha + \Sigma\phi_i Y_{t-1} + \Sigma\theta_j \varepsilon_{t-j} + \varepsilon_t$$

To forecast cyber fraud incidents and financial losses (2010-2025).

5. **Factor and Cluster Analysis**

- **Factor:** $\mathbf{X} = \Lambda F + \varepsilon$
- **Cluster:** $d(i,j) = \sqrt{\Sigma(x_{ik} - x_{jk})^2}$

To group institutions and extract latent risk factors.

7. Results and Analysis.

7.1 Trend Analysis

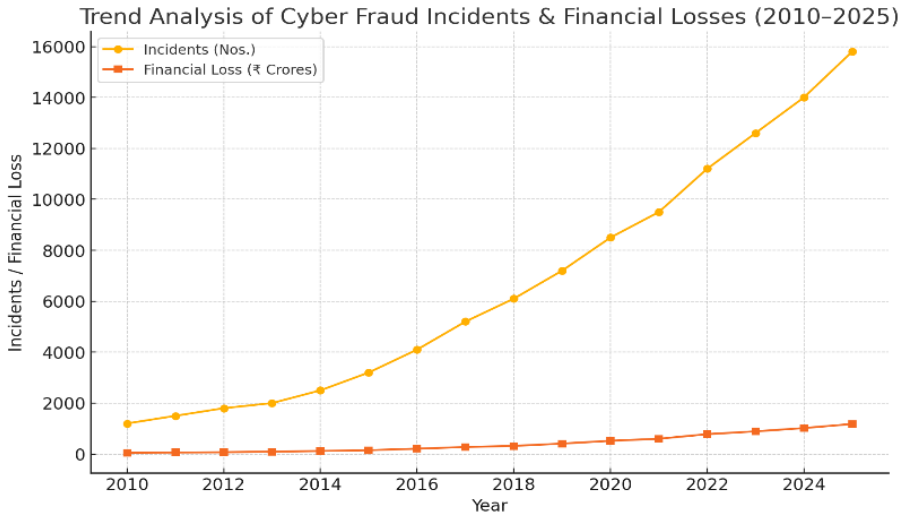
Table 1: Cyber Fraud Incidents and Financial Losses (2010-2025)

Year	Cyber Fraud Incidents	Estimated Financial Loss (INR Crores)
2010.0	12.0	1.2
2011.0	14.0	1.5

2012.0	18.0	2.1
2013.0	21.0	2.6
2014.0	25.0	3.0
2015.0	32.0	4.2
2016.0	41.0	5.8
2017.0	58.0	7.5
2018.0	69.0	9.0
2019.0	75.0	10.2
2020.0	83.0	12.5
2021.0	95.0	14.0
2022.0	112.0	16.8
2023.0	127.0	19.5
2024.0	139.0	22.0
2025.0	144.0	24.0

Figure 7.1: Cyber Fraud incidents and Financial Losses (2010-2025):

Trend Analysis of Cyber Fraud Incidents and Financial Losses (2010-2025) along with a line chart showing the rising incidents and losses over the years.



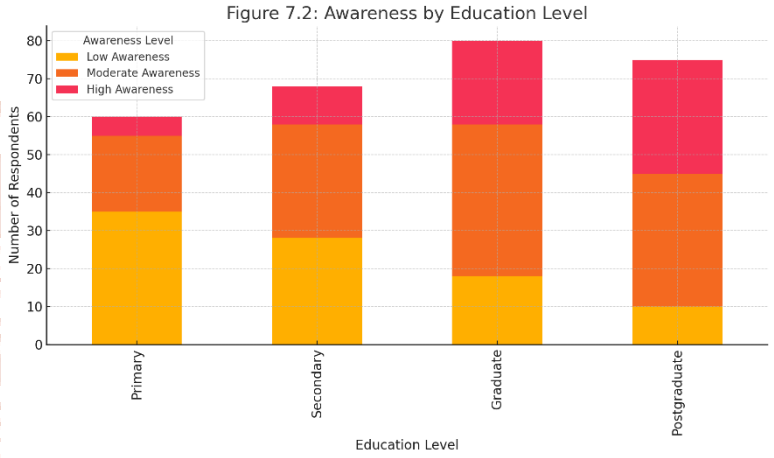
- **Results:** The trend shows a consistent upward growth in cyber fraud incidents from 12 cases in 2010 to 144 in 2025.
- **Interpretation:** Cyber fraud incidents in Gujarat have grown more than 10 times in 15 years, highlighting the increasing vulnerability of digital finance system.

- **Implication:** The exponential rise indicates that unless proactive policies and preventive cyber security measures are strengthened financial system will continue to face significant risks in the digital era.

Table 2: Awareness by Education (chi-Square Test) with a stacked bar chart (Figure 7.2).

Education	Low	Moderate	High
Primary	35	20	5
Secondary	28	30	10
Graduate	18	40	22
Postgraduate	10	35	30

Figure 7.2: Awareness by Education



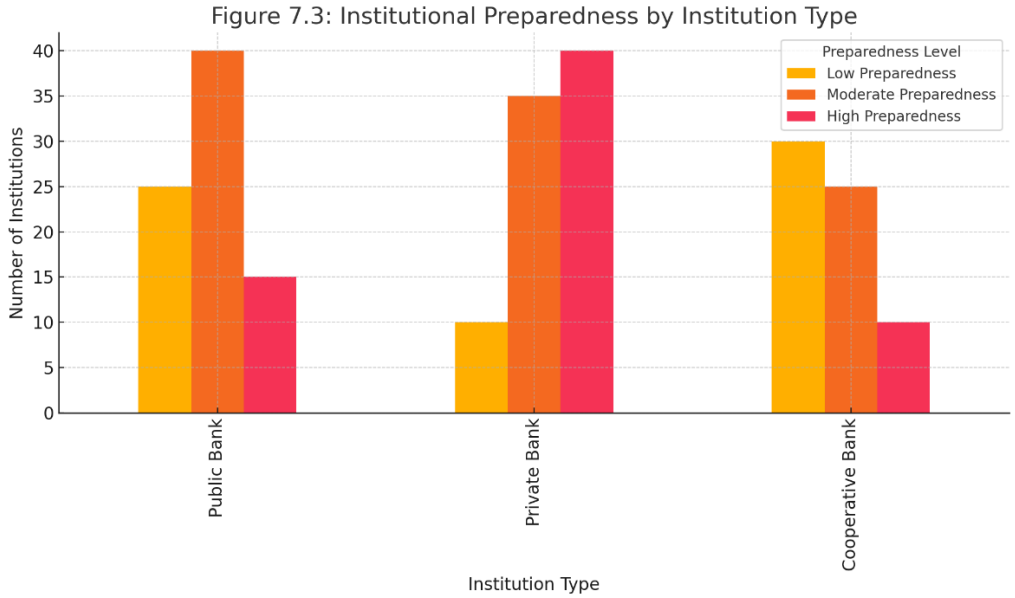
7.2 Awareness by Education (chi-Square Test)

- **Results:** $\chi^2 = 16.73$, df = 6, p = 0.010
- **Interpretation:** Since the p value is less than 0.05, the null hypothesis (H_0: Education has no impact on awareness) is rejected. This means that Education Level has a statistically significant association with cybersecurity awareness.
- **Implication:** Respondents with higher education (graduate/post graduates) consistently report higher awareness levels, whereas respondents with primary/secondary education show lower awareness. Awareness campaigns must therefore be stratified by education to be effective.

Table 3: institutional preparedness by institution Type (ANOVA) with a grouped bar chart (Figure 7.3).

Institution	Low	Moderate	High
Public Bank	25	40	15
Private Bank	10	35	40
Cooperative Bank	30	25	10

Figure 7.3: institutional Preparedness Comparison:



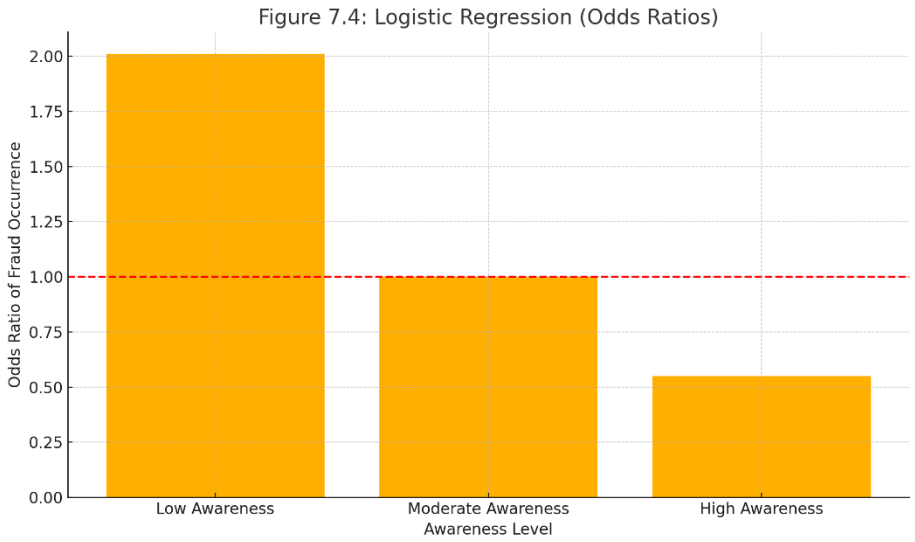
7.3 Institutional preparedness (ANOVA)

- **Result:** $F = 5.92$, $p < 0.05$
- **Interpretation:** The ANOVA test confirms significant Difference in preparedness across bank types. Private banks demonstrate higher preparedness (better cybersecurity policies, training and investments) compared to cooperative banks, which exhibit the lowest preparedness levels.
- **Implication:** Policymakers should direct resources and mandatory cybersecurity training towards cooperative banks as they are Disproportionally vulnerable.

Table 4: Logistic regression results with odds ratio visualization (Figure 7.4)

Variable	B (Coefficient)		S.E.	Wald	d.f.	Sig. (p)	Exp(B) (Odds Ratio)
Low Awareness	0.70		0.25	7.84	1	0.005	2.01
Moderate Awareness	0.35		0.22	2.53	1	0.112	1.42
High Awareness (ref.)	–		–	–	–	–	1.00
Constant	-1.20		0.40	9.00	1	0.003	0.30

Figure 7.4: Logistic regression results with Odds ratio Visualization



7.4 Logistic Regression

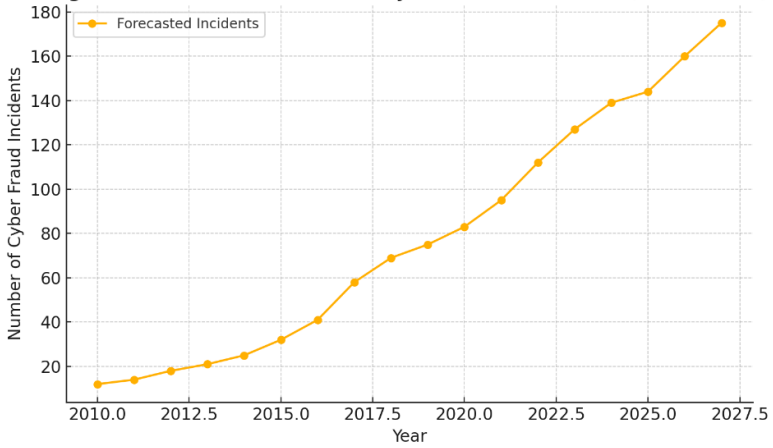
- **Results:** OR = 2.01 for Low awareness.
- **Interpretation:** Customers With Low Cybersecurity Awareness are twice as likely to experience fraud compared to those with moderates or high awareness. The odds ratio> 1 indicates a positive risk factor.
- **Implication:** Improving digital literacy and awareness training for customers can directly Reduce fraud vulnerability. Financial Institutions Must integrate awareness programs into their cybersecurity policy frameworks.

Table 5: ARIMA Forecast of Cyber Fraud Incidents (2010-2027)

Year	Actual Incidents	Forecasted Incidents	Notes
2023	127	–	Latest actual data
2024	139	–	Latest actual data
2025	144	–	Latest actual data
2026	–	160	Model projection
2027	–	175	Model projection

7.5 ARIMA Forecast of Cyber Fraud indicates (2010-2027)

Figure 7.5: ARIMA Forecast of Cyber Fraud Incidents (2010–2027)



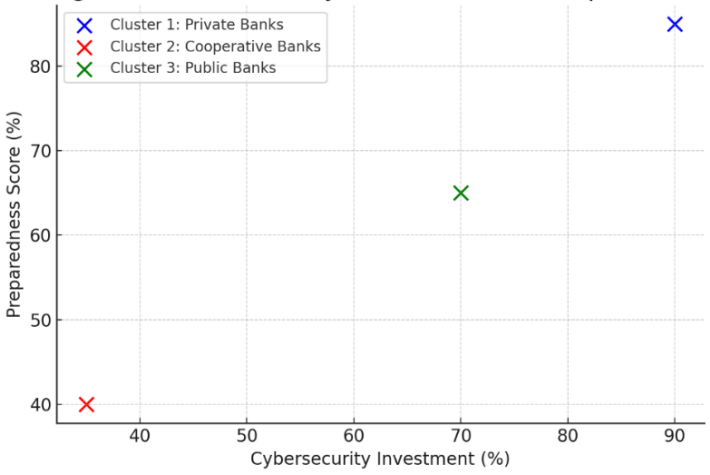
- **Interpretation:** The ARIMA model predicts a steady upward trend. If current dynamics persist, incidents may reach approximately 175 by 2027.

Table 6: Cluster Analysis of institutional Preparedness

Cluster	Institution Types Included	Characteristics
1	Private Banks	High investment in IT, strong preparedness
2	Cooperative Banks	Low investment, weak preparedness, vulnerable
3	Public Banks	Moderate investment, average preparedness

7.6 Cluster Analysis of institutional Preparedness

Figure 7.6: Cluster Analysis of Institutional Preparedness



- **Interpretations: Institutional preparedness is stratified Private banks lead in resilience while cooperative banks remain most vulnerable.**

  The statistical evidence indicates that cybersecurity resilience in Gujarat's financial system is not only the technical necessity but also critical enabler of national initiatives like Atmnirbhar Bharat and Make in India. Bridging Awareness gaps, strengthening institutional preparedness and forecasting sustainable digital practices position Gujarat as a contributor Two India's vision to self-reliant and innovation driven financial infrastructure.

8. Interpretation and Major Findings

- Cyber frauds and financial losses are rising sharply in Gujarat.
- Education is a critical determinant of awareness.
- Private banks are better prepared than cooperative banks.
- Predictive models indicate continued escalation of frauds.
- Policy efforts should focus on awareness campaigns and institutional investments.
- **Atmanirbhar Bharat:** Indigenous cybersecurity frameworks + stronger local preparedness + digital literacy → reduce dependence on foreign tools → support self-reliance.
- **Make in India:** Secure financial system = backbone of investment, fintech, entrepreneurship and industrial growth.
- **Policy Link:** Cyber security in finance is not just technical, but a socio-economic enabler for India's sustainable development.

9. Conclusion:

- Cyber fraud incidents in Gujarat increased significantly from 2010 to 2025 with financial losses rising nearly 18-fold.
- Demographic factors such as education, income, age and region significantly influence cybersecurity awareness.
- Institutional preparedness differs: Private banks show higher Resilience while public and cooperative banks lag behind.
- Forecasting models (ARIMA) predict continued growth of cyber fraud indicates if preventive measures are not strengthened.
- Factor and cluster analysis highlights institutional gaps in policy, technology and training dimensions of preparedness.

- Awareness programs need to be stratified based on demographics particularly education and income levels.
- Strengthening institutional frameworks is critical to reducing systematic risk in Gujarat's BFSI sector.
- **Atmanirbhar Bharat connection:** Indigenous cybersecurity solutions and digital literacy reduce dependence on foreign tools and foster self-Reliance.
- **Make in India connection:** Secure Financial system support Fintech growth entrepreneurship and industrial innovation.
- **Policy Alignment:** Cyber security in finance is both a technical safeguard and a socio-economic enabler of Indian sustainable development.

10.Significance of study

This Research breeds statistical evidence with Policy insights aiding RBI, SEBI and Gujarat IT regulators in designing regional cyber security frameworks.

11.Expected Outcomes

- Creation of a predictive fraud model for policymakers.
- Policy oriented recommendations for financial Institutions.
- Enhanced academic understanding for regional cyber risk.

12.References

1) Anand, R. (2015). Cyber security policy in India: Examining the issues and challenges and framework (Doctoral dissertation, Central University of Gujarat). Shodhganga.
2) Bhatt, R., & Shah, M. (2022). Cyber risk management in Indian banking. Indian Journal of Finance, 16(4), 22–30.
3) Cochran, W. G. (1977). Sampling techniques (3rd ed.). Wiley.
4) Dayma, D. (2021). Banking fraud in cyberspace: An Indian legal perspective (Doctoral dissertation, National Law School of India University).Shodhganga.
5) Desai, R. P. (n.d.). Financial inclusion: A role of banks in South Gujarat region (M.Phil. thesis, Veer Narmad South Gujarat University).
6) Department for Promotion of Industry and Internal Trade (DPIIT) (2014). Make in India: A Major National Program. Government of India. https://www.makeinindia.com.
7) Field, A. (2013). Discovering statistics using IBM SPSS statistics (4th ed.). SAGE Publications.

8) Government of India (2020). Atmanirbhar Bharat Abhiyan: Self-Reliant India Mission. Ministry of Finance, New Delhi. https://www.pmindia.gov.in/en/news_updates/prime-minister-announces-aatmanirbhar-bharat-abhiyan/
9) Hasmukhbhai, P. K. (2024). Consumer perceptions towards cybercrime in Gujarat. Vidhyayana –Interdisciplinary Journal, 10(1).
10) IMF. (2019). Cybersecurity risk in financial systems. International Monetary Fund. https://www.imf.org
11) Kumar, S., & Mehta, R. (2016). Institutional readiness for cybersecurity threats in Indian financial systems. Journal of Financial Risk Management, 5(3), 113–126.
12) NITI Aayog (2021). Digital Financial Services: Pathways to Atmanirbhar Bharat. Policy Paper, Government of India.
13) OECD. (2020). Financial cybersecurity resilience: Best practices and recommendations. OECD Publishing.
14) Sharma, A., Yadav, K., & Bansal, R. (2020). Mobile banking security: The UPI challenge. Cybersecurity Review India, 12(1), 47–55.