

Hacking-Related Cybercrime in Solapur District: An Empirical Analysis of Victim Characteristics and Financial Loss

¹Ms. Anyapanawar Rohini Rahul, ²Mr. Patil Parmeshwar Madhukar, ³Ms. Sutar Shravani Ravikant

¹Assistant Professor, Department of Management & Computer Science, Sangameshwar College, Solapur (Autonomous)

²Assistant Professor, Department of Statistics, Sangameshwar College, Solapur (Autonomous)

³Undergraduate Student, Department of Statistics, Sangameshwar College, Solapur (Autonomous)

Article Info	ABSTRACT
Article History: Received: 17th April 2026 Accepted: 19th April 2026 Published: 21st April 2026 Keywords: <i>Online Investment Fraud, Cyber Crime, Financial Loss, Digital Investment, Share Trading Fraud, Financial Literacy, Cybersecurity</i>	The rapid expansion of digital financial services, online trading platforms, and electronic payment systems has significantly transformed investment practices across the world. While these technological developments have enhanced financial inclusion and accessibility, they have simultaneously increased the incidence of cyber-enabled investment fraud. Online investment scams involving fraudulent trading platforms, fake brokerage applications, cryptocurrency schemes, and social media-based investment promotions have emerged as one of the fastest-growing categories of cybercrime in India. This study investigates the socio-economic characteristics associated with financial losses among victims of online investment fraud using empirical data obtained from officially reported cybercrime cases. The analysis is based on 77 victim records collected from a Cyber Police Office in Maharashtra, India. The dataset includes demographic characteristics, educational qualifications, occupation, residential area, transaction methods, complaint mechanisms, and monetary losses. Descriptive statistical techniques and Chi-square tests of independence were employed to examine the distribution of victims and the association between socio-economic variables and financial loss categories. The findings reveal that middle-aged individuals and salaried employees constitute the largest proportion of victims. Credit/debit cards and Unified Payments Interface (UPI) transactions were the dominant payment modes used in fraudulent transactions. Chi-square analysis indicated no statistically significant association between demographic variables and financial loss categories. The study concludes that online investment fraud is a complex phenomenon influenced by behavioural, technological, and situational factors beyond traditional demographic characteristics. The findings provide important implications for policymakers, financial regulators, law enforcement agencies, and digital payment service providers in strengthening cybercrime prevention strategies, enhancing financial literacy, and promoting secure digital investment practices.

Plagiarism Check Report:

Tool Used: Turnitin

Date of Report: April 17, 2026

Similarity Index: 4%

Remarks: No significant matching text. All citations and matches are properly referenced. The manuscript is considered original.

Copyright © 2026 The Author(s). This is an open access article distributed under the Creative Commons Attribution License, (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

How to Cite: Anyapanawar R. R., et al. (2026). Hacking-Related Cybercrime in Solapur District: An Empirical Analysis of Victim Characteristics and Financial Loss. *IIP: International Multidisciplinary Research Journal (IIPIMRJ)*, 3(II), 23–28.

1. Introduction

The rapid digital transformation of financial services has fundamentally changed the way individuals invest, save, and manage financial assets. The widespread adoption of internet banking, mobile payment systems, online brokerage platforms, and digital investment applications has significantly increased public participation in financial markets. In India, increasing internet penetration, smartphone usage, and government initiatives promoting digital payments have accelerated the growth of online financial transactions and investment activities. While these technological advancements have enhanced financial inclusion and accessibility, they have also created new opportunities for cybercriminals to exploit investors through fraudulent investment platforms, fake trading applications, phishing websites, and deceptive social media promotions. Fraudsters often promise exceptionally high returns with little or no risk, persuading victims to invest substantial amounts before disappearing with the funds.

Online investment fraud has emerged as one of the fastest-growing categories of cybercrime in India. The increasing popularity of digital investment options, including stock market trading, cryptocurrency investments, and online portfolio management, has expanded the scope for financial fraud. To strengthen cybercrime prevention and reporting, the Government of India has introduced several initiatives, including the National Cyber Crime Reporting Portal (NCRP), the Cyber Crime Helpline (1930), and specialized cybercrime investigation units. Despite these measures, the number of reported online investment fraud cases continues to increase, resulting in significant financial losses and undermining public confidence in digital financial services.

Although cybercrime has received increasing attention from researchers and policymakers, empirical studies based on official victim records remain limited, particularly in the context of online investment fraud. Most existing research focuses on the prevalence of cybercrime, awareness levels, or preventive measures, while comparatively fewer studies examine the socio-economic profile of victims using administrative data. Understanding the demographic and socio-economic characteristics of victims is essential for identifying vulnerable groups and developing targeted awareness and prevention strategies.

The present study seeks to examine the socio-economic characteristics of victims of online investment fraud using official cybercrime records obtained from a Cyber Police Office in Maharashtra, India. Using descriptive statistical techniques and Chi-square tests of independence, the study analyses demographic characteristics, educational qualifications, occupation, residential area, transaction methods, complaint mechanisms, and financial loss categories. The findings are expected to contribute to a better understanding of victim characteristics and provide evidence that can assist policymakers, financial institutions, law enforcement agencies, and cybersecurity practitioners in designing more effective fraud prevention policies, financial literacy programmes, and cyber awareness initiatives.

2. Literature Review

Previous studies have examined cyber-enabled financial crime from technological, behavioural, economic, and criminological perspectives. Levi and Smith (2021) argued that technological innovation has fundamentally transformed financial crime, enabling cybercriminals to exploit digital communication channels and online investment platforms. Button and Cross (2022) reported that middle-aged individuals with stable income and active digital banking habits were more vulnerable to investment scams due to behavioural biases such as overconfidence and optimism. Cross (2023) identified social media platforms such as WhatsApp, Telegram, Facebook, and Instagram as major channels facilitating fraudulent investment schemes. The Reserve Bank of India highlighted increasing complaints related to unauthorized digital payments, fake trading platforms, and phishing attacks, recommending stronger authentication systems and enhanced consumer awareness. The Indian Cyber Crime Coordination Centre (I4C) observed that investment-related cybercrime is among the fastest-growing categories of digital fraud in India, with criminals increasingly using fake investment applications and impersonation techniques. Behavioural finance theories, particularly Prospect Theory, suggest that individuals often make investment decisions based on perceived gains rather than objective probabilities, thereby increasing vulnerability to fraudulent investment opportunities. Existing literature also emphasizes that demographic characteristics, digital literacy, and awareness of cybersecurity practices influence victimization, highlighting the need for empirical studies based on official cybercrime records.

3. Research Gap

Existing studies primarily focus on cybersecurity technologies, digital payment security, and behavioural aspects of fraud. Limited empirical investigations have analysed official cybercrime victim records to understand the socio-economic profile of victims and patterns of financial loss associated with online investment fraud. Most studies rely on questionnaire-based surveys rather than official administrative records. Furthermore, demographic characteristics, payment methods, and digital literacy have generally been examined independently rather than within a comprehensive analytical framework. This study attempts to bridge this gap by analysing official cybercrime records using descriptive statistical techniques and Chi-square tests of independence.

4. Objectives of the Study

1. To examine the socio-economic profile of victims of online investment fraud.
2. To analyse patterns of financial losses arising from online investment fraud.
3. To investigate associations between demographic characteristics and financial loss categories.
4. To examine the relationship between selected socio-economic variables and online investment fraud characteristics using Chi-square tests of independence.
5. To provide policy recommendations for reducing cyber-enabled investment fraud.

5. Research Hypotheses

H₀₁: Gender and financial loss category are independent.

H₀₂: Residential area and financial loss category are independent.

H₀₃: Occupation and complaint mode are independent.

H₀₄: Educational qualification and financial loss category are independent.

6. Research Methodology

The study is based on official cybercrime records obtained from a Cyber Police Office in Maharashtra, India. The sample consists of 77 victims who reported incidents of online investment fraud. The collected data include demographic characteristics, educational qualifications, occupation, residential area, transaction methods, complaint mechanisms, and financial loss information. The analysis aims to describe the characteristics of victims and examine associations between selected categorical variables.

Statistical Techniques:

- Frequency distributions
- Percentages
- Mean
- Median
- Standard Deviation
- Histograms
- Box plots
- Chi-square Tests of Independence

The data were analysed using appropriate statistical software. Descriptive statistics were used to summarize the socio-economic characteristics of victims and the distribution of financial losses. Chi-square tests of independence were employed to examine the association between selected categorical variables, including gender and financial loss category, residential area and financial loss category, occupation and complaint mode, and educational qualification and financial loss category.

7. Results and Analysis

7.1 Descriptive Statistics of Financial Loss

Statistic	Value
Sample Size	77
Mean	₹63,669
Median	₹34,000
Standard Deviation	₹105,811
Minimum	₹4,500

Interpretation

The mean financial loss (₹63,669) was substantially higher than the median (₹34,000), indicating a **positively skewed distribution**. This suggests that although most victims experienced moderate losses, a few respondents suffered exceptionally high financial losses, increasing the overall average.

7.2 Chi-Square Test of Independence

The Chi-square test was used to examine the association between selected demographic characteristics and financial loss categories (or complaint mode). The null hypothesis was rejected when $p < 0.05$.

Summary of Chi-square Results

Hypothesis	χ^2	df	p-value	Decision
Gender $\times$ Financial Loss Category	5.837	3	0.120	Not Significant
Residential Area $\times$ Financial Loss Category	3.285	3	0.350	Not Significant
Occupation $\times$ Complaint Mode	0.931	3	0.818	Not Significant
Educational Qualification $\times$ Financial Loss Category	1.633	6	0.950	Not Significant

Interpretation

All p-values exceeded the 0.05 significance level. Therefore, the null hypothesis was accepted for each test, indicating **no statistically significant association** between:

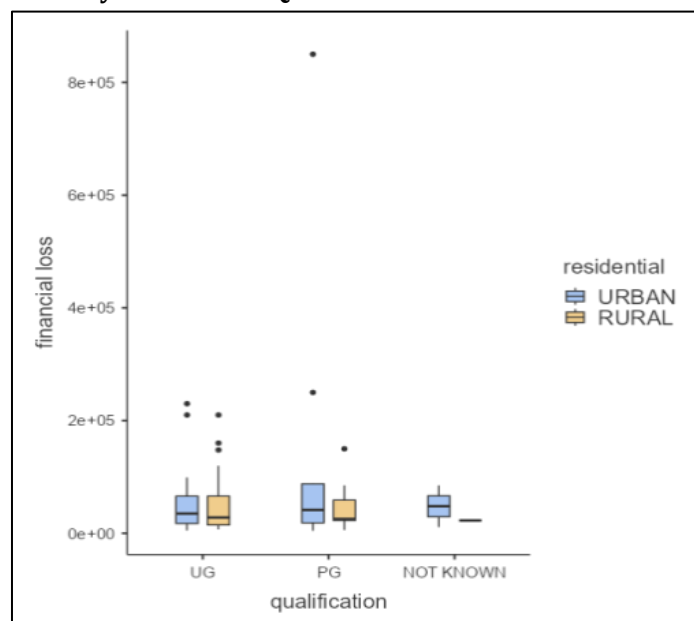
- Gender and financial loss category
- Residential area and financial loss category
- Occupation and complaint mode
- Educational qualification and financial loss category

These findings suggest that financial losses and complaint-reporting behavior were broadly similar across the demographic groups included in the study.

Research Findings

The Chi-square analysis revealed that **none of the selected socio-demographic variables** (gender, residential area, occupation, and educational qualification) had a statistically significant relationship with either financial loss category or complaint mode ($p > 0.05$). Consequently, the study suggests that demographic characteristics alone were not significant determinants of the financial losses experienced by victims of online investment fraud within the sampled population.

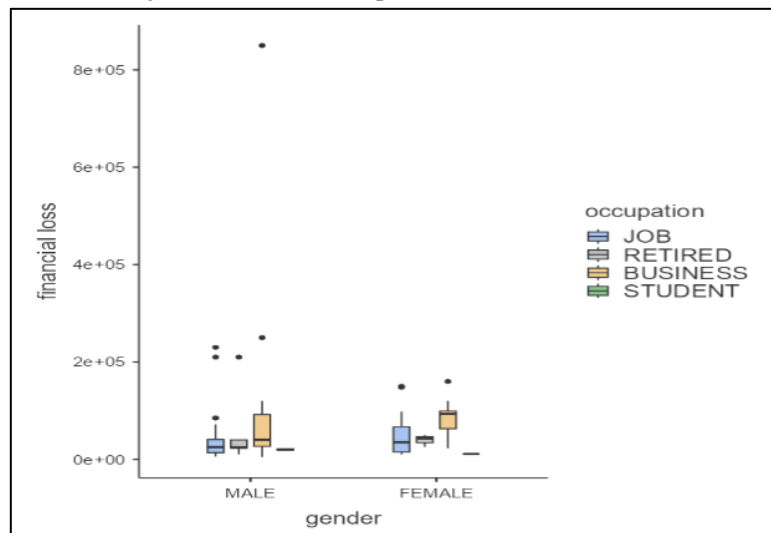
1.Box Plot of Financial Loss by Educational Qualification and Residential Area



Conclusion:

The box plot indicates no substantial difference in financial loss between urban and rural respondents across educational qualification groups. Although a few outliers and higher variability are observed among postgraduate respondents, no consistent pattern is evident.

2. .Box Plot of Financial Loss by Gender and Occupation



Conclusion:

The box plot shows that financial loss varies across occupational groups, with higher variability observed in the Business category. Despite a few extreme outliers, particularly among males, no clear association between gender, occupation, and financial loss is evident.

8. Conclusion

The present study examined the socio-economic characteristics of victims of online investment fraud using official cybercrime victim records from Maharashtra, India. The findings revealed that middle-aged, salaried, and graduate individuals constituted a larger proportion of the victims. However, the Chi-square tests indicated no statistically significant association between demographic characteristics such as gender, residential area, occupation, and educational qualification and financial loss categories.

The findings suggest that online investment fraud is a complex phenomenon influenced by behavioural, technological, and situational factors rather than traditional socio-economic characteristics alone. Factors such as financial literacy, investment behaviour, fraud sophistication, digital awareness, and psychological susceptibility are likely to play an important role in shaping victimization and financial losses. The study contributes to the growing body of empirical evidence on cyber-enabled financial crime and provides useful insights for policymakers, financial institutions, law enforcement agencies, and regulatory authorities in designing targeted awareness programmes, strengthening cybersecurity measures, and developing evidence-based strategies to reduce online investment fraud.

9. Limitations of the Study

The study has the following limitations:

The analysis was based on a relatively small sample of 77 officially reported cybercrime victim records, which may limit the generalizability of the findings.

Data were obtained from a single Cyber Police Office in Maharashtra; therefore, regional variations in cyber fraud patterns were not captured.

Only selected socio-economic variables were available in the administrative records, while important behavioural and psychological factors such as financial literacy, investment experience, risk perception, trust, and fraud awareness were unavailable.

The study employed a cross-sectional dataset, which does not permit examination of changes in victim behaviour over time.

The analysis was limited to descriptive statistical techniques and Chi-square tests of independence. Additional behavioural, technological, and contextual variables may provide a more comprehensive understanding of online investment fraud.

10. Future Scope

Future research may extend the present study by:

Using larger and multi-state datasets to improve the generalizability of the findings.

Incorporating behavioural finance variables, digital literacy, cyber awareness, investment experience, and psychological characteristics to better understand victimization and financial loss.

Applying advanced machine learning and artificial intelligence techniques for fraud detection, pattern recognition, and cybercrime prevention.

Conducting longitudinal studies to examine trends in online investment fraud and changes in victim behaviour over time.

Comparing different categories of cyber fraud, such as investment scams, cryptocurrency fraud, phishing attacks, loan application fraud, and digital arrest scams.

Developing comprehensive risk assessment frameworks that assist cyber police, financial institutions, and regulatory authorities in identifying emerging fraud patterns and strengthening preventive measures.

11. References

- Button, M., & Cross, C. (2022). *Cyber fraud and victimisation in the digital economy*. Routledge.
- Cross, C. (2023). Online investment scams and the evolving cybercrime landscape. *Journal of Financial Crime*, 30(2), 401–418.
- Indian Cyber Crime Coordination Centre (I4C). (2023). *Annual Report on Cyber Crime in India*. Ministry of Home Affairs, Government of India.
- Levi, M., & Smith, R. G. (2021). Fraud and cyber-enabled financial crime: Emerging trends and policy responses. *Crime, Law and Social Change*, 75(4), 413–430.
- Organisation for Economic Co-operation and Development (OECD). (2022). *OECD Digital Economy Outlook 2022*. OECD Publishing.
- Reserve Bank of India. (2023). *Annual Report 2022–23*. Reserve Bank of India.
- Reserve Bank of India. (2023). *Report on Trend and Progress of Banking in India 2022–23*. Reserve Bank of India.
- Securities and Exchange Board of India. (2023). *Investor Awareness and Protection Initiatives*. SEBI.
- World Bank. (2022). *World Development Report 2022: Finance for an Equitable Recovery*. World Bank.
- Ministry of Home Affairs, Government of India. (2023). *National Cyber Crime Reporting Portal: Annual Statistics*. Government of India.