SCIENTIFIC CULTURE
www.sci-cult.com

*SCIENTIFIC CULTURE, Vol. 12, No. 4, (2026), pp. 2859-2866*
*Open Access. Online & Print*

**DOI: 10.5281/zenodo.12426356**

# DIGITAL FINANCIAL LITERACY AND AWARENESS RELATED TO DIGITAL FINANCIAL FRAUD

**Urvi Amin[1*], Suzan Peters[2], Dhreeti Amin[3]**

*[1]Department of Management, Shri Jairambhai Patel Institute of Business Management (NICM), Gandhinagar, Gujarat, India.*
*[2]MBA (Finance), Department of Management, Shri Jairambhai Patel Institute of Business Management (NICM), Gandhinagar, Gujarat, India.*
*[3]B.A. (Economics), Department of Economics, St. Xavier's College, Ahmedabad, Gujarat, India*

*Received:* **13/09/2025**
*Accepted:* **21/02/2026**

*Corresponding Author: Urvi Amin (urviamin@ymail.com)*

## ABSTRACT

***Financial literacy and financial awareness play a significant role in the digital world. Financial inclusion has been improved by government programs like the Jan Dhan–Aadhaar–Mobile (JAM) trinity to spread financial literacy and awareness, which changed the overall financial services industry. Researchers look at how financial literacy and awareness boosted society's confidence in using digital payments. The impact of the rising risk of digital financial fraud in India's quickly digitizing economy is examined in this study. Among the methods by which financial services can reach the general public and are closely associated with digitalization are digital wallets, blockchain, UPI, and mobile banking. Cyber fraud and harassment will result from minor errors or a failure to follow protocol. The major objective of this research study is to identify factors that are responsible for digital fraud. 250 respondents who faced this digital fraud through technovation, analysed with Structure Equation Model- SEM based on exploratory research method. Using primary data collection techniques, this study seeks to examine the relationships among financial literacy, digital financial literacy, digital payment usage, cybersecurity awareness, and fraud vulnerability. Research shows poor digital hygiene stems from a lack of knowledge. The study's findings demonstrated a robust positive relationship between the variables and their effects. Even though digital payments are becoming more and more popular, especially among youth, many users still lack the basic knowledge required to manage cyber risks. The study's conclusions indicate that increasing financial literacy and awareness is crucial to reducing the risk of digital fraud and enabling the safe use of digital financial services. A secure, inclusive, and robust digital financial ecosystem necessitates collaboration among the government, financial institutions, and educators.***

**KEYWORDS:** Cybersecurity Awareness, Digital Financial Literacy, Digital Financial Fraud, Digital Payment, Financial Literacy, SEM.

## 1. INTRODUCTION

Fatemeh Kimiyaghalam and Stanley Yap (2017) proposed that *financial literacy encompasses the knowledge and ability to make informed and effective decisions regarding financial resources. It represents the intersection of financial, credit, and debt management, along with the understanding required to make prudent or financially responsible choices.* A deficiency in financial literacy results in an ineffective participation in the financial inclusion framework. The distribution of benefits to the populace is predominantly problematic in a nation like India. One notable advantage of a scheme initiated by the Modi administration is the direct transfer of subsidies for LPG, which has received considerable appreciation. Financial literacy will facilitate improved decision-making and the efficient management of funds. Understanding the fundamentals of time value can lead to the development of a strong portfolio. As reliance on digital infrastructure grows, data breaches have emerged as a significant concern for organizations globally. Despite comprehensive research in the field of cybersecurity, there is a scarcity of studies that have investigated the external factors affecting an organization's susceptibility to data breaches. The process of digitalization is transforming the landscape of the financial sector.

Cybercrime is "any unlawful act where computer or communication device or computer network is used to commit or facilitate the commission of crime," according to the National Cyber Crime Reporting Portal. Cybercrimes could be defined as theft of identity, social media linked attacks, digital banking scams, cyberattacks through mobile apps, virus attacks and psychological tactics. Cybercrime includes online drug trafficking, vishing, smishing, digital wallet robbery, credit/debit card skimming, morphing of photos, online sextortion, cyber bullying, cyber stalking, phishing, cyber terrorism, cyber espionage, data stealing, website defacement, cybersquatting, pharming, cryptojacking, hacking social media accounts, and more. Saneja, K., & Kumar, A. (2024). To Study on Cyber Crime Burgeoning in India and Crucial Actions Need for Every Cybercrime Victim. In 2025, India is ranked 10th in the World Cybercrime Index amongst 194 countries, named Global Cybersecurity Index (GCI), which is published by the International Telecommunication Union (ITU) to assess and rank countries based on their commitment to cybersecurity.

## 2. LITERATURE REVIEW

Ashraf, N. (2024) aims to explore India's efforts to strengthen its cyberspace from the post-independence era to the present, focusing on domestic measures, policies, and collaborations to enhance cyber resilience and reduce dependence on foreign technology. The study employs secondary data from official documents, including India's policies like the New Electronics Policy, IT Act 2000, and National Cyber Security Policy. It also analyzes the roles of key entities such as the National Informatics Centre, CERT-In, and Defence Cyber Agency, and examines bilateral and multilateral collaborations.

Singh, P., & Singh, H. (2024) explores the critical role of cybersecurity in enhancing India's internal security, examining the increasing vulnerabilities and threats in cyberspace as digital technologies become integral to governance, infrastructure, and daily life. The study analyzes the evolving nature of cyber threats and their potential impact on critical sectors like finance, healthcare, energy, and defence.

C., A. C. (2024). The article examines India's evolution in cybersecurity and data privacy, from the Information Technology Act of 2000 to the Digital Personal Data Protection Act of 2023, analyzing key legislative developments and their implications on securing digital assets, particularly in the banking sector. The study employs an analytical and qualitative approach, primarily utilizing primary and secondary literature. It provides a descriptive case explanation of cybersecurity in banking, highlighting legislative measures, committee formations, and judicial interventions.

Bhardwaj, A. (2024) India's security landscape is increasingly complex, with growing threats from both domestic and transnational terrorism, cyber-attacks, extremism, and environmental crises. To effectively counter these threats, India must focus on improving intelligence capabilities, inter-agency collaboration, and bolstering its cybersecurity and counterterrorism infrastructure.

Tripathy, S. S. (2024) analyses the role of public awareness, cybersecurity education, and regulatory frameworks in combating cybercrime. The surge in cybercrime in India, particularly in sectors like banking, healthcare, and government, underscores the vulnerability of individuals and organizations to digital threats. Increasing internet penetration and digital payment adoption have heightened exposure to cyber risks. To address these challenges, the paper highlights the need for innovative prevention strategies, enhanced internal security protocols, and stronger regulatory frameworks to safeguard sensitive data and digital infrastructure.

Naik, R. L., Jain, S., & Manjula, B. (2024) examines the intersection of cybersecurity and sustainability,

emphasizing the role of robust cybersecurity measures in achieving the United Nations' Sustainable Development Goals (SDGs), with a specific focus on India, where rising cyber threats pose significant challenges.

Shukla, S., Kant, R., Srivastava, C., Gautam, A., & Yadav, P. (2024) suggested that organizations should prioritize cyber resilience alongside security, involving cybersecurity experts in leadership roles and also global collaboration and a unified legal framework are essential to combat cyber terrorism. The authors concluded that in India, secure platforms for key sectors and fast implementation of the National Cyber Security Strategy are urgently needed as well as strengthening laws, dedicated cyber courts, and increased investment in cyber defence will help minimize cybercrime effects and support economic growth.

Kocurek, S., &Maniam, B. (2022). To analyze corporate financial fraud, its evolving nature, and the role of regulations and policies in fraud detection and prevention. A qualitative analysis of corporate fraud schemes, regulatory frameworks, and preventive measures, focusing on fraud detection, governance, and whistleblowing mechanisms. Corporate fraud affects all industries, requiring continuous regulatory adaptation. Fraud prevention relies on governance, detection techniques, and whistle-blower protections. If unchecked, fraud can harm corporations, individuals, and economic growth.

Sharma, A. K. (2024) employs a comprehensive literature review and case study analysis. It examines definitions, classifications, and preventive strategies across different institutional perspectives, comparing approaches in India and globally. The research highlights the growing prevalence of online fraud, especially with the rise of digital transactions during COVID-19. Financial institutions implement measures like two-factor authentication and customer awareness campaigns, but evolving fraud tactics require continuous adaptation. Collaboration among stakeholders and robust security frameworks are crucial to mitigating risks and minimizing financial losses.

Sunderajulu, K. B. (2024) aims to examine the security challenges in digital payment transactions, analyzing the effectiveness of existing technologies, regulatory frameworks, and user-centric approaches in mitigating fraud and risks. The research employs a qualitative and analytical approach, reviewing existing literature, regulatory guidelines, and industry standards. It explores technological advancements such as cryptographic protocols, tokenization, and compliance with frameworks like PCI-DSS, PSD2/SCA, and RBI regulations.

Shukla, A., & Kashni, T. (2024) aims to evaluate the research developments related to banking frauds and scams by analyzing existing literature and identifying gaps in the field. A bibliometric analysis of 288 studies published up to August 4, 2024, was conducted using Scopus and VOS viewer software. The analysis examined key authors, influential papers, funding institutions, and affiliations.

Roy, N. C., &Sreeleakha, P. (2024) the complex nature of cyber fraud and emphasizes the need for proactive rather than reactive mitigation strategies. It introduces a unique approach that treats each cyber fraud as a distinct "fraud event," integrating early warning signs for timely intervention. This framework enhances the banking sector's ability to manage cyber risks, ensuring stability, reputation protection, and improved risk management.

Mehta, A. (2024) explores the impact of technological advancements on banking frauds in India, analyzing their evolving nature, vulnerabilities, and strategies for mitigation. A qualitative approach is adopted, including a review of banking fraud tactics such as phishing, malware attacks, identity theft, and social engineering.

Jain, S., Sharma, J., Sharma, S., Kaushik, A., & Rajawat, N. (2024) highlights that Fintech has significantly disrupted traditional banking, offering innovative, efficient, and customer-friendly solutions. However, this shift has also increased exposure to financial cybercrimes. The research identifies key areas of concern, including cybersecurity threats, fraud risks, and regulatory challenges. The findings emphasize the need for strong security frameworks, collaboration between banks and Fintech firms, and continuous innovation in fraud prevention mechanisms.

Rajput, R. S., & Thakral, B. (2024) explores digital payment solutions such as UPI, BHIM, and mobile wallets are widely available, low digital literacy remains a significant barrier to adoption. Rural consumers face issues such as lack of awareness, cybersecurity concerns, and inadequate banking infrastructure. The findings emphasize the need for targeted financial literacy programs, improved digital infrastructure, and stronger security measures to enhance digital payment adoption in rural India.

## 3. RESEARCH OBJECTIVES

### *3.1. Primary Objectives*

**H1:** Digital Awareness is associated with Perception in digital financial transactions.

**H2:** Fraud Exposure is associated with Fraud Response behavior.

**H3:** Fraud Response is associated with Usage Behavior.

## 4. RESEARCH METHODOLOGY

Using a quantitative explanatory design, this study investigates the relationship between digital awareness, perception, exposure to fraud, response to fraud, and usage behavior in relation to digital finance. Using convenience sampling via online questionnaire, data collection was done from digital transaction user in India. Validated Likert scales with multiple items were used to measure constructs. Data analysis was done by method of Structure Equation Model. The measurement model (reliability, convergent, and discriminant validity) and structural model (path coefficients, significance, and $R^2$) were assessed by PLS-SEM in SmartPLS 4 software to test the H1–H3 hypotheses based on exploratory research method. The results were examined by considering p-value less than 0.05 is significant.

Most scholars studying digital fraud and financial literacy have done so separately. This research study evaluates digital literacy, exposure, reaction to fraud, and usage behaviours based on the same model. Data was collected from 250 users of digital finance services in India through online surveys with scaled measures for all constructs, using PLS-SEM to explore relationships, predict outcomes, and manageable to small sample sizes (Chin 1998; Hair et al. 2019). Discriminant validity was assessed using HTMT which stands for Heterotrait–Monotrait Ratio of Correlations (Henseler et al. 2015), with a level of significance of $p < 0.05$. Usefulness of this study is based on measuring the above factors simultaneously, thus providing further understanding of how digital financial service operators can reduce fraud.

## 5. DATA ANALYSIS BY IMPLEMENTATION OF SEM MODEL

### *5.1. Measurement Model Assessment*

In PLS-SEM, the measurement model is evaluated by utilising following components.

***Table 1: Outerloadings- Matrix***

| | AW | FO | FR | P | PCF | UB |
|---|---|---|---|---|---|---|
| AW6 | 0.703 | | | | | |
| AW7 | 0.915 | | | | | |
| FO3 | | 1.000 | | | | |
| FR5 | | | 0.969 | | | |
| FR6 | | | 0.949 | | | |
| P2 | | | | 1.000 | | |
| PCF4 | | | | | 1.000 | |
| UB3 | | | | | | 0.909 |
| UB4 | | | | | | 0.859 |

The measurement model demonstrates strong indicator reliability, as all outer loadings exceed the recommended threshold of 0.70. Particularly, AW7 (0.915), FR5 (0.969), and UB3 (0.909) indicate substantial convergent strength within their respective constructs. This confirms indicator reliability and suggests that all measurement items strongly represent their respective latent constructs. The single-item constructs (FO, P, PCF), exhibiting loadings of 1.000, were theoretically justified due to their specific and narrowly defined conceptual representation. The use of single-item constructs is justified when the construct is concrete, unidimensional, and directly observable (e.g., specific fraud occurrence types or primary concern indicators).

The measurement model demonstrated satisfactory reliability and discriminant validity. All indicator loadings exceeded the recommended threshold of 0.70, confirming indicator reliability

### *5.2. Discriminant Validity*

To evaluate data suggested that Discriminant validity ensures constructs are distinct from each other. In this test through HTMT ratio and Cross Loading.

***Table 2: Discriminant validity - Heterotrait-monotrait ratio (HTMT) - Matrix***

| | AW | FO | FR | P | PCF | UB |
|---|---|---|---|---|---|---|
| AW | | | | | | |
| FO | 0.108 | | | | | |
| FR | 0.125 | 0.249 | | | | |
| P | 0.556 | 0.205 | 0.103 | | | |
| PCF | 0.186 | 0.164 | 0.045 | 0.100 | | |
| UB | 0.151 | 0.178 | 0.157 | 0.286 | 0.051 | |

### *B. Cross Loadings*

*Table 3: Discriminant validity - Cross loadings*

| | AW | FO | FR | P | PCF | UB |
|---|---|---|---|---|---|---|
| AW6 | 0.703 | 0.110 | 0.107 | 0.240 | -0.079 | 0.025 |
| AW7 | 0.915 | -0.019 | 0.038 | 0.422 | -0.142 | 0.129 |
| FO3 | 0.033 | 1.000 | 0.240 | 0.205 | 0.164 | 0.150 |
| FR5 | 0.084 | 0.246 | 0.969 | 0.124 | 0.012 | 0.159 |
| FR6 | 0.056 | 0.212 | 0.949 | 0.065 | 0.071 | 0.089 |
| P2 | 0.425 | 0.205 | 0.103 | 1.000 | -0.100 | 0.241 |
| PCF4 | -0.143 | 0.164 | 0.039 | -0.100 | 1.000 | -0.046 |
| UB3 | 0.098 | 0.125 | 0.129 | 0.202 | -0.062 | 0.909 |
| UB4 | 0.095 | 0.143 | 0.105 | 0.228 | -0.014 | 0.859 |

The HTMT ratios were well below 0.85, establishing discriminant validity among constructs. Cross-loading analysis further confirmed that each indicator loaded highest on its intended construct. HTMT ratios ranged from 0.045 to 0.556, well below the conservative threshold of 0.85, confirming discriminant validity. This suggests that respondents clearly distinguished between awareness, perception, fraud occurrence, post-fraud response, and behavioural adaptation constructs.

### *5.3. Structural Model – Effect Size ($f^2$)*

Effect size ($f^2$) indicates how strongly an exogenous variable influences an endogenous variable. **Rule (Cohen, 1988) suggested that,** 0.02 = Small, 0.15 = Medium and 0.35 = Large considered.

*Table 4: f-square – Matrix*

| | AW | FO | FR | P | PCF | UB |
|---|---|---|---|---|---|---|
| AW | | | | 0.221 | 0.013 | |
| FO | | | 0.061 | | | |
| FR | | | | | | 0.018 |
| P | | | | | 0.002 | |
| PCF | | 0.028 | | | | |
| UB | | | | | | |

AW → P ($f^2$ = 0.221, $R^2$ for P = 0.181)

While awareness significantly influences perception, the downstream effects (e.g., FO → FR, FR → UB) demonstrate relatively small effect sizes. This suggests that fraud experience alone may not automatically translate into behavioural transformation or preventive adaptation. The relatively low $R^2$ values for FO, FR, and UB suggest that digital fraud dynamics are influenced by additional contextual and psychological factors beyond awareness and perceived complexity. Future models may incorporate trust, digital literacy depth, institutional response effectiveness, or socio-demographic moderators to enhance explanatory power. In the structural model, AW exhibited a moderate effect on P ($f^2$ = 0.221), suggesting meaningful predictive relevance. However, other relationships showed small to negligible effect sizes, indicating limited practical influence among those constructs...

Given the increasing relevance of digital literacy in financial ecosystems, awareness is expected to shape users' cognitive evaluation of digital transactions. However, the strength and practical magnitude of this relationship remain empirically underexplored in emerging digital contexts.

H1: Digital Awareness is associated with Perception in digital financial transactions.

Awareness → Perception (AW → P)

The path between Digital Awareness and Perception was examined using bootstrapping procedures. The relationship demonstrated moderate practical relevance ($f^2$ = 0.221). The model explains 18.1% of the variance in Perception ($R^2$ = 0.181), suggesting modest explanatory power in line with exploratory modelling objectives.

H2: Fraud Exposure is associated with Fraud Response behavior. Fraud Exposure → Fraud Response (FO → FR)

Experiential exposure to fraud incidents may influence behavioural response mechanisms. However, the extent to which exposure translates into structured response behavior remains conceptually uncertain, particularly in emerging digital environments.

The effect of Fraud Exposure on Fraud Response was found to be small in magnitude ($f^2$ = 0.061). The model explains only 5.8% of the variance in Fraud Response ($R^2$ = 0.058), indicating limited predictive strength. This suggests that direct exposure alone may not be sufficient to drive structured response

behavior, reinforcing the exploratory nature of the model.

H3: Fraud Response is associated with Usage Behavior.

Fraud Response → Usage Behavior (FR → UB)

Behavioural adaptation theories suggest that response mechanisms may influence subsequent digital usage patterns. Nevertheless, empirical validation in the context of digital fraud remains limited.

The relationship between Fraud Response and Usage Behavior exhibited negligible effect size ($f^2$ = 0.018), with the model explaining only 1.8% of the variance in Usage Behavior ($R^2$ = 0.018).The weak explanatory power suggests that post-fraud response may not substantially alter digital transaction behavior, indicating the presence of unobserved influencing factors.

Overall, while the measurement model demonstrated strong reliability and discriminant validity, the structural model exhibited modest explanatory capability. These findings align with exploratory SEM objectives, where the emphasis lies on identifying preliminary structural patterns rather than confirming high predictive strength.

AW → P (moderate effect)

Cognitive awareness demonstrates comparatively stronger influence than experiential exposure mechanisms in shaping digital financial perception.

The exploratory structural analysis indicates that awareness-related constructs exhibit comparatively stronger practical influence relative to exposure-driven mechanisms. Although overall predictive power remains modest, the findings provide preliminary evidence that cognitive preparedness may play a more central role than experiential victimization in digital fraud-related behavioural modelling. The framework does not assume deterministic causality but instead examines potential structural associations among constructs to identify preliminary behavioural patterns within the digital financial ecosystem**.**

## 6. FINDINGS

The structural model results indicate that digital awareness exerts a moderate and meaningful influence on perceived fraud-related capability ($f^2$ = 0.221; $R^2$ = 0.181), confirming H1. This suggests that awareness initiatives significantly enhance individuals' confidence in managing digital financial risks.

In contrast, the effect of fraud exposure on post-fraud response behavior is small ($f^2$ = 0.061), providing limited support for H2. While exposure to fraud triggers some reactive measures, its practical influence appears modest.

Similarly, the relationship between post-fraud response and preventive behavioural adaptation demonstrates a negligible effect ($f^2$ = 0.018), indicating weak support for H3. This suggests that reactive responses do not strongly translate into long-term preventive behavioural transformation.

Researchers have concluded that while cognitive preparedness is very dependent on awareness, there is little evidence that changed behaviours in regard to preventing white collar crime will result from having previously been a victim of fraud. This suggests that to effectively adapt to future incidents, fraud victims will require proactive which is rather than implementing reactive responses.

### *6.1. Finding related to Policy Implications*

As such, interventions aimed at prevention should be much more heavily focused on providing awareness based opportunities than on taking any form of reactive action after an incident has occurred. Both the Reserve Bank of India and the governing bodies for digital payments can provide structured literacy programs that focus on how to identify and report fraud. Financial institutions can provide proactive digital literacy training via online modules, rather than relying solely on grievance redressed processes. Furthermore, establishing a simplified cyber-crime reporting framework will enable individuals who experience fraud to continue engaging with their institutions post-incident, highlighting the impact of this research on society.

The data demonstrates that digital awareness is critical for influencing perceived capacity to control and mitigate digital financial risk. Furthermore, the link between being a victim of fraud and changing one's behavior related to risk mitigation is weak i.e., awareness provided through cognition has a greater influence on behavior than factors associated with experiential learning, and implying that future policy recommendations should be directed toward proactive awareness programs and structured institutional engagement with individuals who experience frauds rather than depending only on learning from experience of the frauds they have experienced.

## 7. CONCLUSION NOTE

According to this research, individuals' digital awareness is an important factor in how capable they feel to use a digital financial system. The gap between experience with fraud and the transition to taking preventative steps against it was weak, which

indicates that just having experience with fraud is not enough to create enduring preventative behavior.

The results of this research suggest that policies should emphasize proactive digital literacy (DL) programs and built-in institutional support systems, rather than depend solely on corrective action after the fact (post fraud). In the later behaviour stages, limited behaviour change would indicate the need for additional factors for example digital confidence, institutional effectiveness, and perceived seriousness) to be included in any more studies.

The study demonstrated a clear gap between having a history of fraud and the implement of changed behaviour argues that having a fraud history is unlikely to create the motivation to engage in preventative behaviour. Therefore, there is a strong requirement for institutional confidence, credible enforcement, and perceived effectiveness of enforcement to assist individuals in adjusting to the consequences of their fraud experiences.

This study encompassed four constructs: digital financial awareness, experiences with fraud, and responses to fraud after experiencing fraud, and taking preventative measures against fraud. Using SEM modelling, the findings provide significant insight into the combined impact of knowledge and experience on individual's behaviour toward online fraud.

## MANAGERIAL INSIGHT

This research demonstrates a new distinction in previous digital fraud studies as it distinguishes between experience-driven change (adaptation) and awareness-driven thought process (cognitive). Although many past studies concluded that being a victim of fraud would impact future behaviours to prevent becoming a future victim; this study finds a clear cause and effect between awareness, knowledge of their experience, reaction to their perception of their experience, and ultimately adapt to the repeated fraud experience. The authors emphasize that the ability to build a fraud resilient person is based not on previous experience, but rather on having developed a strong level of cognitive awareness. The authors suggest that organizations should devote resources toward building digital literacy (awareness) through education rather than expect that people will be able to reactively compensate (prevent) for previous fraud experiences.

Ultimately, digital awareness influences behaviours that support fraud-resilience; while fraud experiences may drive reactive behaviours; structured awareness is the greatest driver of proactive adaptation. Developing strong cognitive readiness for any future fraud opportunities will be critical in developing sustainable digital financial infrastructures.

## LIMITATIONS

This study has few limitations. First, the use of cross-sectional survey data makes it difficult to establish causal relationships between any two variables. Second, participants may create social desirability bias in their responses because they self-report their answers. Third, measuring fraud exposure as binary (yes or no) means that some aspects of participants' experiences will not be captured. Finally, the small sample size of N=251 limits the generalizability of the results.

## FUTURE RESEARCH DIRECTIONS

Future researchers can expand upon this study by: using longitudinal studies to assess the trajectory of participants' prevention behaviours; taking into consideration psychological factors, such as digital trust or technological self-efficacy; comparing multiple countries in order to assess how regulation impacts fraud prevention; and using mixed-methods designs like combining survey and interview or case study methods to elaborate on participants' perceptions of fraud.

## REFERENCES

Ashraf, N. (2024). India’s cyber landscape: an assessment of Indian efforts since independence. Journal of Contemporary Studies, 108–123. https://doi.org/10.54690/jcr.2023(xii-ii).13772

Bhardwaj, A. (2024). India’s Cybersecurity Journey. Advances in Hospitality, Tourism and the Services Industry (AHTSI) Book Series, 159–180. https://doi.org/10.4018/979-8-3693-2715-9.ch009

Bulko, H. (2024). Fraud and corruption as an object of internal audit in corporate governance. Ekonomìka, Fìnansi, Pravo. https://doi.org/10.37634/efp.2024.3.25

C., A. C. (2024). Strengthening India’s Cybersecurity and Data Privacy Landscape: A Comprehensive Overview. Indian Journal of Public Administration, 70(3), 466–478. https://doi.org/10.1177/00195561241271616

Jain, S., Sharma, J., Sharma, S., Kaushik, A., & Rajawat, N. (2024). Bibliometric Analysis of Literature on Fintech and Cyber Frauds in Banking. 138–144. https://doi.org/10.1201/9781003543633-22

Jhunjhunwala, S. (2023). Internal Control, Financial Oversight and Risk Management (pp. 73–99). https://doi.org/10.1007/978-981-99-2707-4_4

Kocurek, S., &Maniam, B. (2022). Corporate financial fraud. Journal of International Finance and Economics, 22(1), 65–75. https://doi.org/10.18374/jife-22-1.5

Mehta, A. (2024). Impact of technological advancements on banking frauds: A case study of Indian banks. International Journal of Research in Finance and Management. https://doi.org/10.33545/26175754.2024.v7.i1c.308

Naik, R. L., Jain, S., & Manjula, B. (2024). Navigating Sustainability in Cyber Security: Challenges and Solutions. 147–164. https://doi.org/10.2174/9789815256680124010012

Nejad, M. G., &Sabzian, H. (2024). Spatiotemporal patterns of consumer financial fraud in the United States. International Journal of Bank Marketing. https://doi.org/10.1108/ijbm-01-2024-0023

Rajput, R. S., & Thakral, B. (2024). Challenges in Digital Payments and Financial Cyber Frauds in Rural India. 56–69. https://doi.org/10.2174/9789815238990124010006

Roy, N. C., &Sreeleakha, P. (2024). Proactive cyber fraud response: a comprehensive framework from detection to mitigation in banks. Digital Policy, Regulation and Governance. https://doi.org/10.1108/dprg-02-2024-0029

Sharma, A. K. (2024). An Analysis of Online Monetary Fraud and the Application of Marketing Strategies by Indian Banks to Mitigate Fraudulent Activities: A Literature Review. Journal of Informatics Education and Research, 4(3). https://doi.org/10.52783/jier.v4i3.1931

Shukla, A., & Kashni, T. (2024). Bibliometric analysis of banking frauds and scams literature. Journal of Financial Crime. https://doi.org/10.1108/jfc-08-2024-0252

Singh, P., & Singh, H. (2024). The Crucial Role of Cyber Security in Safeguarding India's Internal Security. International Journal of Science and Research. https://doi.org/10.21275/sr24102131723

Sunderajulu, K. B. (2024). eCommerce & Digital Wallet Payment Fraud. Deleted Journal, 2(6). https://doi.org/10.62127/aijmr.2024.v02i06.1111

Tian, J., & Sun, H. (2023). Corporate financialization, internal control and financial fraud. Finance Research Letters, 56. https://doi.org/10.1016/j.frl.2023.104046

Tripathy, S. S. (2024). A comprehensive survey of cybercrimes in India over the last decade. International Journal of Science and Research Archive, 13(1), 2360–2374. https://doi.org/10.30574/ijsra.2024.13.1.1919