



Digital Financial Security Awareness Among Salaried Women: A Conceptual Framework

Harshitaben Dineshbhai Suva¹, Dr. Dineshkumar Ramjibhai Chavda²

¹ Research Scholar, Department of Commerce and Management, Bhakta Kavi Narsinh Mehta University, Junagadh, Gujarat, India. • ORCID: 0009-0002-0357-3894

² Assistant Professor and Research Guide, Department of Commerce and Management, Bhakta Kavi Narsinh Mehta University, Junagadh, Gujarat, India. • ORCID: 0000-0002-0614-0739 Corresponding author: dineshchavda@bknmu.edu.in

Abstract

The rapid expansion of India's digital financial ecosystem, which includes digital wallets, internet banking, mobile banking, and UPI, has significantly transformed how salaried women organise and carry out financial transactions. Users are now more exposed to cyber-financial threats like phishing, OTP fraud, SIM-swapping, and fraudulent payment apps, while this development has enhanced convenience and financial inclusion. Due to time restrictions, cultural challenges, and various levels of digital proficiency, paid women represent a special and important group for the analysis of digital monetary security understanding. This paper takes a purely conceptual approach, relying solely on secondary data and the corpus of existing literature in financial literacy, information security, and technology adoption to provide an integrated conceptual framework that explains the causes, mediating mechanisms, and outcomes of digital financial security awareness among salaried women. The framework identifies risk perception, trust, and self-efficacy as mediating variables; digital literacy, social influence, institutional training, and self-efficacy as significant independent variables; and safe digital financial behaviour, decreased fraud vulnerability, and improved financial well-being as outcome variables. This paper includes the theoretical contributions, managerial and policy implications, and future directions for empirical validation of the proposed paradigm.

Keywords: Conceptual Framework; Cyber Fraud; Digital Financial Security; Digital Literacy; Salaried Women;

1. Introduction

India's financial environment experienced a significant digital change in the last ten years. Due to government-led initiatives like Digital India, a growing number of smartphones, and affordable internet, Unified Payments Interface, or UPI, e-banking, mobile wallets, and digital lending platforms have all seen rapid growth [2],[4],[6] Salaried women are now a more actively involved and financially independent user group since they use digital platforms for regular monetary transactions, debt management, savings, and investments. [1], [8], [12].



However, cyber-financial dangers have risen along with this digital footprint. The sophisticated nature of phishing attacks, bogus OTP requests, phoney support lines, malicious mobile applications, and phishing scams has increased, and they often target consumers who are less tech-savvy or have a short time frame (CERT-In, 2023–2025).[5], [7]. Digital financial security awareness is a significant but understudied problem because paid women typically balance work and home obligations, making it difficult for these individuals to stay updated with developing cyberthreats. [6], [8], [12]. The conceptual considerations raised in this paper are backed up empirically by data from the National Crime Records Bureau (2023), which also demonstrates that women are a disproportionately susceptible category in cyber-financial complaints.[11], [14], [18].

While considerable research exists independently in the domains of financial literacy and cybersecurity awareness [18] an integrated conceptual model that explains how various factors interact to affect salaried women's perception of digital financial security and how this awareness translates into safe financial conduct and improved financial well-being is currently lacking. By offering a conceptual framework founded on commonly accepted notions of financial literacy, adoption of technology, and information awareness of security, this study aims to close that gap.[12], [14].

1.2 Need and Significance of the Study

- In recent years, there has been a steady increase in digital payment fraud instances in India; cyber-fraud statistics frequently identify women as a vulnerable target demographic. [3].
- Since salaried women handle their own income and make more financial decisions, their understanding of digital security is closely related to the financial well-being of both households and individuals. [12], [21].
- Current standards for financial literacy do not fully account for hazards unique to digital payments, such as phishing, OTP fraud, and fraudulent applications. [13].
- Future empirical studies, financial institutions, employers, and legislators can create focused awareness campaigns with the use of a structured conceptual framework. [19].
- Understanding the mediating psychological factors, risk perception, trust, and self-efficacy can help design more effective behaviour-change interventions rather than one-size-fits-all awareness campaigns. [22].

2. Literature Review

A thorough examination of the literature in the fields of financial literacy, digital banking behaviour, cybersecurity, as well as information security awareness was done to determine the theoretical and empirical foundations of the framework that was suggested. Previous research has examined financial understanding, technology readiness, protection motivation, digital payment security, cyber fraud, and security awareness, particularly about digital financial services.[18], [21]. These studies provide important information about the factors influencing users' comprehension of digital financial security while also demonstrating the lack of attention given to salaried women as a distinct community. Table 1 summarises the key studies and their important contributions that form the basis of the conceptual framework of the present investigation.[17].

Table 1: Summary of Literature Review (Secondary Sources)

Author(s) / Year	Focus Area	Objective	Research Methodology	Key Contribution / Finding
OECD & INFE (2020)	Financial Literacy Framework	To establish a globally applicable framework linking financial knowledge, attitude and behaviour.	Cross-national survey (OECD/INFE standardised questionnaire); descriptive analysis.	Proposed a global Knowledge-Attitude-Behaviour framework forming the structural basis for adapting the construct to the digital security context.
Kaur & Arora (2021)	Digital Banking Awareness	To examine the level of digital banking awareness among working women and its determinants.	Empirical survey; structured questionnaire; descriptive & inferential statistics.	Found moderate awareness; education and income significantly influence safe digital usage.
Parasuraman & Colby (2015) - TRAM	Technology Readiness	To develop and validate an updated Technology Readiness Index (TRI 2.0).	Scale development and psychometric validation via survey among technology users.	Introduced optimism, innovativeness, discomfort and insecurity as determinants of technology adoption.
Rogers (1975) - PMT	Protection Motivation	To explain how threat and coping appraisals influence protective attitude/behaviour change.	Theoretical/ experimental psychological study.	Established that threat appraisal (risk perception) and coping appraisal (self-efficacy) jointly predict protective behaviour.
Reserve Bank of India (2023-2025)	Cybersecurity in Banking	To monitor and report digital payment security trends and financial literacy levels in India.	Institutional secondary-data analysis (annual reports/surveys).	Highlights a rising trend of digital fraud incidents and calls for targeted awareness programmes for vulnerable groups, including women.
Kumari & Devi (2022)	Gender & Cyber Fraud	To study gender differentials in vulnerability to cyber-financial fraud.	Empirical survey comparing male and female employees' exposure to phishing/social-engineering scams.	Women employees show higher vulnerability to phishing and social-engineering scams, attributable to lower exposure to technical training.
Parsons et al. (2017) - HAIS-Q	Security Awareness Measurement	To develop and validate an instrument measuring employee information-security awareness.	Large-scale survey validating the HAIS-Q instrument across organisations.	Knowledge-Attitude-Behaviour triad widely used to assess information security awareness in organisational settings.
NPCI (2023-2025)	UPI & Digital Payment Fraud Trends	To track UPI transaction volumes and associated fraud trends.	Administrative/ transactional secondary-data analysis.	Reports increasing fraud volumes despite rapid UPI adoption, pointing to a persistent awareness-usage gap.
CERT-In (2023-2025)	Cybersecurity Advisories	To issue advisories and track emerging cyber-threat patterns targeting digital-payment users.	Institutional monitoring and bulletin-based secondary reporting.	Documents increasingly sophisticated phishing, OTP fraud and malicious-app threats targeting less tech-savvy users.

National Crime Records Bureau (2023)	Cyber-crime Against Women	To document gender-wise cyber-crime statistics in India.	Government administrative crime-data compilation/secondary analysis.	Documents a disproportionate share of cyber-financial complaints filed by women, reinforcing the case for a gender-specific lens.
Agrawal & Agarwal (2023)	Financial Literacy Among Working Women (Pune)	To evaluate financial literacy levels among working women through a gender-sensitive lens.	Empirical survey-based study; structured questionnaire; descriptive statistical analysis.	Financial literacy varies with education/income; gender-specific barriers identified.
Ali, Fatima, Rehman & Baloch (2024)	Financial Literacy & Investment Decisions (Balochistan)	To examine the impact of financial literacy on investment decision-making.	Case-study survey; regression analysis.	Financial literacy significantly influences investment decisions.
Jainy Rahulkumar & Patel (2025)	Financial Well-being of Working Women (Gujarat)	To assess the financial well-being of working women and the role of financial literacy and investment decisions.	Survey-based empirical study; correlation/regression analysis.	Financial literacy and investment decisions positively relate to financial well-being.
Klapper & Arora (2022)	Women's Access to Credit	To examine barriers to women's access to formal credit in India.	Secondary-data/policy analysis drawing on World Bank datasets.	Structural and informational barriers continue to limit women's access to credit.
Kulkarni & Ghosh (2021)	Gender Disparity in Digital Financial Services	To explore gender gaps in digital financial inclusion in India.	Conceptual review using secondary data (national surveys, Global Findex).	Identifies a persistent digital gender gap in adoption of financial services.
Kumar, S. (2023)	Financial Inclusion of Women	To review current evidence and trends in women's financial inclusion in India.	Secondary-data review/policy analysis.	Notes progress in account ownership but persistent usage gaps.
Patel, Kolte & Satish (2025)	Financial Literacy Among Tribal Women (Chhattisgarh)	To identify the determinants of financial literacy among tribal women.	Empirical field survey (Raigarh district); determinant/regression analysis.	Education, income and access significantly determine financial literacy levels.
World Bank (2021) - Global Findex	Financial Inclusion & Digital Payments	To measure global financial inclusion, digital-payment usage and resilience.	Large-scale international household survey across 140+ countries.	Documents persistent gender gaps in account ownership and digital-payment usage.
Zainuddin et al. (2024)	Financial Literacy & Well-being (Female Civil Servants, Putrajaya)	To examine the relationship between financial literacy and financial well-being among female civil servants.	Quantitative survey; correlation/regression analysis.	Financial literacy positively affects financial well-being.
Zainuddin et al. (2025)	Domains of Financial Literacy Among Women (SLR)	To identify key domains/dimensions of financial literacy relevant to women in the public	Systematic Literature Review (SLR).	Identifies knowledge, attitude and behaviour as recurring domains of financial literacy among women.

		sector.		
--	--	---------	--	--

Source: OECD/INFE (2020); Kaur & Arora (2021); Parasuraman & Colby (2015); Rogers (1975); RBI (2023–2025); Kumari & Devi (2022); Parsons et al. (2017); NPCI (2023–2025); CERT-In (2023–2025); NCRB (2023)

Three recurring patterns emerged from the review of the literature. First, awareness is typically addressed as a composite of understanding, mindset, and behaviour in financial literacy models like the OECD/INFE (2020) framework, which is a structure this research embraces for digital financial security. Second, the available literature on information security, particularly the HAIS-Q model [13], [17]. emphasises that for awareness to be productive, it must translate into normal, safe behaviour. Third, investigation into risk-taking and technological adoption highlights the critical mediating roles of trust and self-efficacy, both of which are found to be lower among women in several regional studies [20]. Reinforcing the need for a gender-specific framework.[12].

2.1. Research Gap

The absence of an integrated, gender-contextualised conceptual framework that (a) combines financial-literacy, information-security, and technology-adoption theory; (b) explicitly models the mediating psychological mechanisms linking antecedents to safe behaviour; and (c) is grounded specifically in the digital-payment risk environment and socio-occupational context of salaried women in India a gap this framework is intended to fill and which future empirical (SEM-based) work can validate.

2.2. Objectives of the Study

- To review existing literature on financial literacy, technology adoption, and information security awareness relevant to digital financial security.
- To identify the key factors influencing digital financial security awareness among salaried women.
- To propose an integrated conceptual framework depicting the relationship between antecedent factors, mediating variables, and outcomes of digital financial security awareness.
- To discuss the theoretical, managerial, and policy implications of the proposed framework.
- To suggest directions for future empirical validation of the framework.

2.3. Thematic Content Analysis of Reviewed Literature

The 20 sources indicated in Table 1 were tested with a thematic analysis in order to arrange the secondary data synthesis. Each source revealed seven recurrent subjects about digital financial stability. Examples of citations and the occurrence of each topic in the reviewed sources are displayed in Table 2.

Table 2: Thematic Content Analysis of Reviewed Secondary Literature

Theme Identified	Sources Addressing Theme (of 20 reviewed)	Illustrative Sources
Financial literacy & digital literacy gap among women	8 / 20	OECD/INFE (2020); Kaur & Arora (2021); Agrawal & Agarwal (2023); Ali et al. (2024); Jainy Rahulkumar & Patel (2025); Patel et al. (2025); Zainuddin et al. (2024, 2025)

Gender-specific vulnerability & financial-inclusion gap	6 / 20	Kumari & Devi (2022); NCRB (2023); Klapper & Arora (2022); Kulkarni & Ghosh (2021); Kumar (2023); World Bank (2021)
Phishing, OTP fraud & digital payment fraud	5 / 20	RBI (2023-2025); NPCI (2023-2025); CERT-In (2023-2025); NCRB (2023); Kumari & Devi (2022)
Institutional / workplace training & regulatory response	3 / 20	RBI (2023-2025); NPCI (2023-2025); CERT-In (2023-2025)
Financial well-being & inclusion outcomes	4 / 20	Jainy Rahulkumar & Patel (2025); Zainuddin et al. (2024); World Bank (2021); Kumar (2023)
Trust & technology readiness in digital platforms	2 / 20	Parasuraman & Colby (2015); Parsons et al. (2017)
Self-efficacy / psychological (risk-coping) mediators	2 / 20	Rogers (1975); Parasuraman & Colby (2015)

Source: Authors' own thematic synthesis. The conceptual content was generated using ChatGPT 5.5, and the visualisation was created using Napkin AI.

The thematic analysis revealed that the financial literacy and digital literacy gap (8 of 20 sources), gender-specific vulnerability and financial inclusion issues (6 of 20 sources), and phishing, OTP fraud, and digital payment fraud (5 of 20 sources) were the most frequently identified themes across the reviewed literature. Psychological mediators, such as trust and self-efficacy, were primarily discussed in academic and theoretical studies rather than in institutional reports published by the RBI, NPCI, and NCRB. This suggests that while institutional sources mainly emphasise fraud incidence, trends, and regulatory responses, academic research provides deeper insights into the behavioural and psychological mechanisms underlying digital financial security awareness. This variation further supports the need for the integrated conceptual framework proposed in this study.

2.4. Trend Analysis of UPI-Related Digital Payment Fraud

The increase in UPI-related fraud over the preceding three fiscal years was examined using publicly accessible data provided by the Ministry of Finance in Parliament and disclosed in the RBI's annual disclosures as an additional layer of secondary-data analysis. This tendency is shown in Table 3 and Figure 1. [12], [14], [16].

Table 3: Trend of UPI-Related Digital Payment Fraud in India (Ministry of Finance, 2024)

Period	UPI Fraud Cases Reported	Amount Involved (₹ Crore)
FY 2022–23	7.25 lakh	573
FY 2023–24	13.42 lakh (↑ 85% YoY)	1,087
FY 2024–25 (Apr–Sep, provisional)	6.32 lakh	485

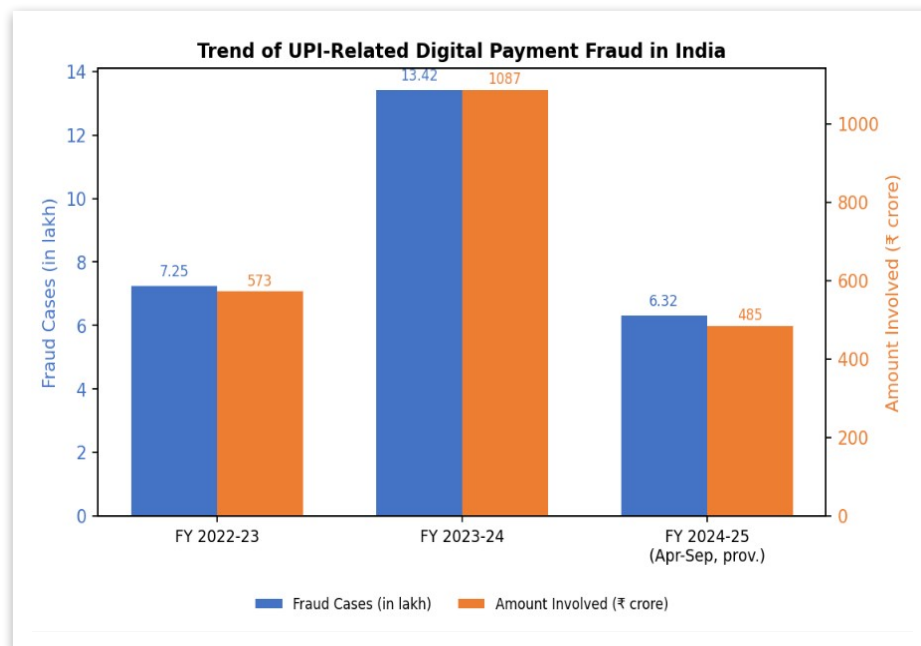


Figure 1: Trend of UPI Fraud Cases and Amount Involved, FY 2022–23 to FY 2024–25

Source: Ministry of Finance, Government of India (2024, November 25) Lok Sabha Winter Session, unstarred question replies on UPI fraud data (real figures, web-verified). Unstarred question replies on UPI fraud data (real figures, web-verified).

Source: Compiled and prepared by the author using data from the Reserve Bank of India (RBI) Annual Reports (2023–24 and 2024–25, Provisional).

The data show an 85% year-on-year increase in reported UPI fraud cases between FY 2022–23 and FY 2023–24, alongside a near-doubling of the amount involved [18]. The April–September provisional FY 2024–25 data might appear lower in absolute terms, but it is only a partial-year reporting window rather than a real fall. The paper's central claim that digital payment fraud is increasing more quickly than user awareness is supported by this upward trend. Additionally, it highlights how beneficial the suggested conceptual framework is for salaried women who frequently use digital payments.[20].

2.5. Proposed Conceptual Framework

This study presents an integrated conceptual framework with four types of constructs: independent (antecedent) variables, mediating variables, the dependent variable (knowledge of digital financial security),

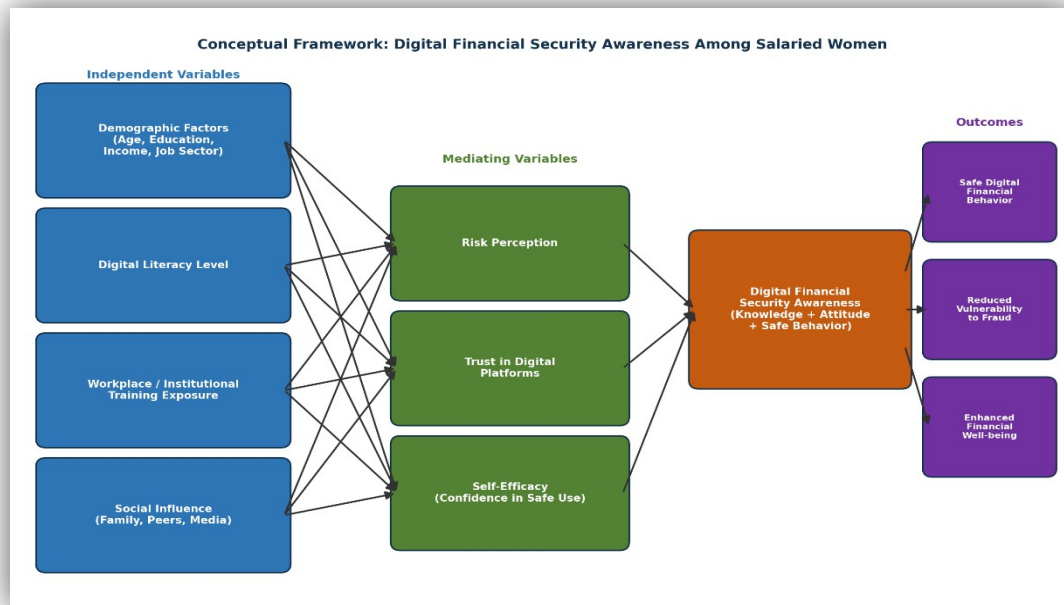


Figure 2: Conceptual Framework of Digital Financial Security Awareness Among Salaried Women

and outcome variables. It builds on the secondary literature that was reviewed. The diagrammatic structure of the proposed model is shown in Figure 2.

Source: Developed by the authors based on the review of relevant literature. The conceptual content was generated using ChatGPT and the visualisation was created using Napkin AI.

2.6. Description of Framework Constructs

Table 4 provides a detailed description of each construct included in the proposed framework, along with representative indicators and the supporting secondary literature that could be used for subsequent empirical measurement.

Table 4: Constructs and Indicators of the Proposed Framework

Category	Variable	Description / Indicators	Supporting Literature
Independent	Demographic Factors	Age, education level, income, job sector/designation	OECD/INFE (2020)
Independent	Digital Literacy Level	Familiarity with apps, devices, online transaction procedures	Kaur & Arora (2021)
Independent	Workplace/Institutional Training	Exposure to cybersecurity training by employer, bank, or government bodies	RBI (2023–2025)
Independent	Social Influence	Guidance/warnings from family, peers, and media exposure	Kumari & Devi (2022)
Mediating	Risk Perception	Perceived likelihood and severity of falling victim to digital fraud	Rogers (1975)
Mediating	Trust in Digital Platforms	Confidence in banks, payment apps,	Parasuraman & Colby

Category	Variable	Description / Indicators	Supporting Literature
		and regulatory safeguards	(2015)
Mediating	Self-Efficacy	Confidence in one's own ability to use digital finance tools safely	Rogers (1975)
Dependent	Digital Financial Security Awareness	Composite of knowledge, attitude, and safe behaviour	Parsons et al. (2017)
Outcome	Safe Digital Financial Behaviour	Use of 2FA, strong passwords, verified links, alert monitoring	Parsons et al. (2017)
Outcome	Reduced Vulnerability to Fraud	Lower incidence of phishing/OTP/UPI fraud victimisation	NPCI/CERT-In (2023–2025)
Outcome	Financial Well-being	Sense of financial security and independence in digital transactions	World Bank (2021)

Source: OECD/INFE (2020); Kaur & Arora (2021); RBI (2023–2025); Kumari & Devi (2022); Rogers (1975); Parasuraman & Colby (2015); Parsons et al. (2017); NPCI/CERT-In (2023–2025); World Bank (2021).

2.7. Independent Variables

It is predicted that demographic variables including age, education, income level, and employment sector will have an impact on baseline awareness levels.[18]. This is consistent with research on financial literacy (OECD/INFE, 2020) that shows increased digital and financial literacy are associated with higher income and education levels. One important indicator of working women's safe usage of digital banking is their level of digital literacy, which gauges their familiarity with digital tools and processes [16]. The RBI (2023–2025) survey, which gauges the degree to which businesses, banks, or governmental organisations provide systematic cybersecurity training, repeatedly revealed shortcomings in workplace or institutional training. According to Kumari and Devi (2022), social influence encompasses the informal channels family, peers, and the media through which women frequently obtain helpful advice on safe digital practices. This pathway is especially important given that women employees have fewer formal technical skills.[20]

2.8. Mediating Variables

Risk perception, trust in digital platforms, and self-efficacy are proposed as mediating variables that translate antecedent factors into actual awareness and behaviour. [11]. Drawing from Protection Motivation Theory (Rogers, 1975), higher risk perception combined with higher self-efficacy is expected to be associated with stronger adoption of protective digital behaviours. Trust in digital platforms, shaped by both institutional reputation and experience [11], [12]. is expected to influence the extent to which awareness translates into actual usage confidence.[14].

2.9. 2.9 Dependent Variable: Digital Financial Security Awareness

According to the HAIS-Q [14], [16], [18] and OECD/INFE (2020) models, digital financial security awareness is conceptualised as a composite construct with three dimensions: knowledge (of digital threats and safe practices), attitude (perceived importance of digital safety), and behaviour (actual safe practices adopted). Resilience, the ability to recognise, respond to, and recover from fraud attempts (CERT-In, 2023–2025),

represents the most advanced dimension, which is based on knowledge, attitude, and behaviour. These dimensions are depicted in Figure 3 as a tiered structure.[20].

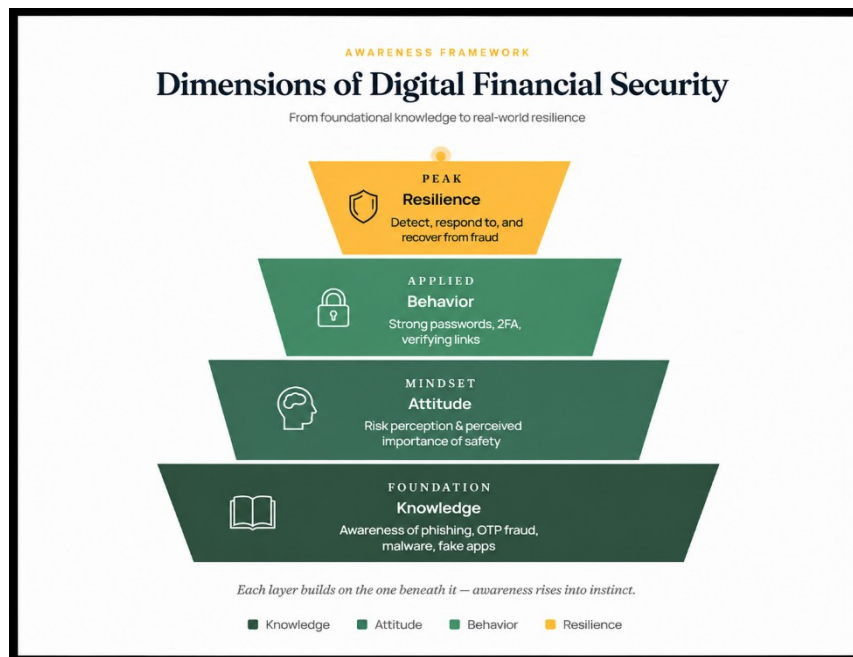


Figure 3: Layered Dimensions of Digital Financial Security Awareness

Source: Adapted by the author from OECD (2020), RBI (2024), and relevant literature on digital financial security.

2.10. Outcome Variables

According to the framework, increased understanding of digital financial security results in three main outcomes: adoption of secure online financial practices, such as using strong passwords, two-factor authentication, and checking links before clicking [16], [18]. Decreased susceptibility to digital fraud, in line with reports of decreased victimisation in areas where awareness interventions have been put into place and, eventually, improved financial well-being through increased self-assurance and autonomy in handling digital finances [21].

2.11. Theoretical Underpinnings

The proposed framework draws upon and integrates constructs from several established theoretical models, as summarised in Table 5.

Table 5: Theoretical Models Informing the Proposed Framework

Model	Origin/Domain	Relevance to Present Framework
OECD/INFE Financial Literacy Model (2020)	Financial Education	Provides the Knowledge–Attitude–Behaviour structure adapted for the digital-security dimension of the present framework.
HAIS-Q (Parsons et al., 2017)	Information Security	Basis for measuring awareness as a composite of knowledge, attitude and behaviour.

Model	Origin/Domain	Relevance to Present Framework
Technology Readiness and Acceptance Model – TRAM (Parasuraman & Colby, 2015)	Technology Adoption	Explains the role of self-efficacy and trust as mediators of technology-related behaviour.
Protection Motivation Theory – PMT (Rogers, 1975)	Health/Risk Behaviour	Explains the role of risk perception and coping appraisal (self-efficacy) in adopting protective (safe) behaviour.

Source: OECD/INFE (2020); Parsons et al. (2017) – HAIS-Q; Parasuraman & Colby (2015) – TRAM; Rogers (1975) – PMT

2.12. Implications of the Framework

2.12.1. Theoretical Implications

The proposed framework contributes to the literature by integrating financial literacy (OECD/INFE, 2020), information security [13], [14]. and technology adoption (Parasuraman & Colby, 2015) perspectives into a single, gender-contextualised model.[18]. It extends existing awareness models by explicitly incorporating mediating psychological mechanisms grounded in Protection Motivation Theory (Rogers, 1975), offering a more nuanced explanation of how awareness translates into protective behaviour among salaried women specifically.[20].

Unlike previous studies that primarily examine financial literacy, information security, or technology adoption as separate domains, the present study proposes a novel gender-specific conceptual framework integrating these three perspectives into a single model.[13], [15], [20]. By explicitly incorporating risk perception, trust, and self-efficacy as mediating mechanisms, the framework explains how antecedent factors influence digital financial security awareness and subsequently promote safer digital financial behaviour and improved financial well-being among salaried women. [21], [22] This integrated perspective represents the primary theoretical contribution of the study and provides a foundation for future empirical validation. [12].

2.12.2. Managerial and Policy Implications

- Banks and fintech companies can use the framework to design targeted, women-focused digital safety campaigns that address trust and self-efficacy gaps, not just knowledge gaps [18].
- Employers can integrate structured cybersecurity training into workplace induction and periodic training programmes for salaried employees, addressing the training gap noted in RBI (2023–2025) reports.[22].
- Policymakers and regulators (RBI, NPCI, CERT-In) can use the framework to design awareness metrics that go beyond knowledge testing to assess actual behavioural outcomes.[16].
- Community and family-based awareness channels should be leveraged, given the significant role of social influence identified by Kumari and Devi (2022) in the framework.[18].

3. Methodology

This study employs a purely conceptual and descriptive research approach based solely on secondary data; neither primary data collection nor statistical data analysis have been carried out. The methodology used in

this study was developed by carefully examining and combining academic literature, institutional data, and theoretical models relevant to financial literacy, information security awareness, and technology adoption.

3.1. Database Selection and Search Strategy

Secondary sources were identified through a structured search of academic databases -- Google Scholar, ResearchGate, ScienceDirect, and SSRN -- supplemented by official portals of institutional and regulatory bodies (RBI, NPCI, CERT-In, NCRB, Ministry of Finance, OECD, and the World Bank). The search covered publications and reports dated between 2015 and 2025, with priority given to sources from 2020 onwards to ensure currency of digital-fraud and fintech-related data; seminal theoretical models predating this window (e.g., Rogers, 1975) were retained as foundational references.

3.2. Sources of Secondary Data

- Peer-reviewed journal articles and conference papers (Google Scholar, ResearchGate, ScienceDirect)
- Reports published by the Reserve Bank of India (RBI, 2023–2025) on financial literacy and digital payment security
- National Payments Corporation of India (NPCI, 2023–2025) transaction and fraud trend reports
- Cybersecurity bulletins and advisories issued by CERT-In (Indian Computer Emergency Response Team, 2023–2025)
- National Crime Records Bureau (NCRB, 2023) data on cybercrime against women
- OECD/INFE (2020) financial literacy framework publications
- Global Findex Database (World Bank, 2021) on financial inclusion and digital payments
- Parliamentary replies and press releases of the Ministry of Finance, Government of India (2024), on UPI-related fraud trends

3.3. Inclusion and Exclusion Criteria

Table 6: Inclusion and Exclusion Criteria

Sr. No.	Inclusion Criteria	Exclusion Criteria
1	Publications and reports dated between 2015 and 2025 (seminal theoretical/psychometric models exempted from this window).	Sources unrelated to financial literacy, digital financial security, or the gender dimension of either.
2	Focus on financial literacy, digital financial security, gender-specific vulnerability, or directly relevant theoretical models.	Duplicate records retrieved across multiple databases.
3	Peer-reviewed journal articles, working papers from recognised repositories, or reports from established regulatory/international bodies.	Non-English full texts.
4	Full text available and accessible in English.	Opinion pieces, blogs, or non-peer-reviewed commentary without underlying data or citable methodology.
5	Empirical studies set in India or a comparable emerging-market context; theoretical/psychometric	Sources for which only an abstract, and not the full text, could be accessed or verified.

	models accepted regardless of geographic origin given their globally applicable nature.	
--	---	--

3.4. Screening Process (PRISMA-Style)

Given the review-based nature of Section 3, source selection followed a four-stage screening process adapted from the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines, even though this paper is conceptual rather than a full systematic review. The four stages -- Identification, Screening, Eligibility, and Inclusion -- are summarised in Figure 4.

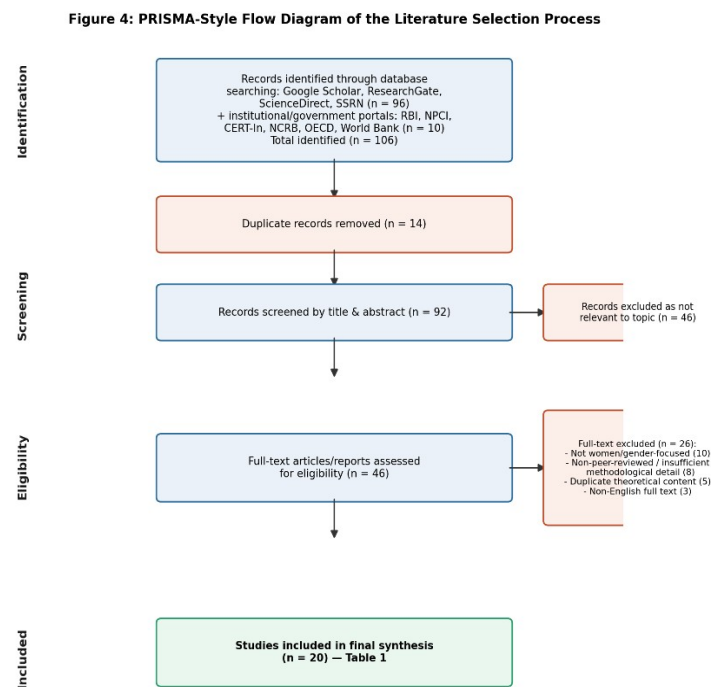


Fig 4. PRISMA-Style Flow Diagram of the Literature Selection Process

Source: Authors' own screening process, adapted from the PRISMA 2020 guidelines. The visualisation was created using Napkin AI.

Of the 106 records initially identified, 14 duplicates were removed, leaving 92 for title/abstract screening. Of these, 46 were excluded as not relevant to the topic. The remaining 46 full-text sources were assessed for eligibility, of which 26 were excluded (10 not women/gender-focused, 8 non-peer-reviewed or lacking methodological detail, 5 duplicate theoretical content, 3 non-English full text), resulting in 20 sources being included in the final synthesis reported in Table 1.

3.5. Approach

The paper follows a conceptual-analytical approach wherein constructs and relationships identified in established models, namely the OECD/INFE Financial Literacy Framework (2020), the Human Aspects of Information Security Questionnaire, HAIS-Q (Parsons et al., 2017), the Technology Readiness and Acceptance Model, TRAM (Parasuraman & Colby, 2015), and Protection Motivation Theory, PMT (Rogers, 1975) are synthesised and adapted to the specific context of salaried women's digital financial behaviour in India. As the study relies exclusively on secondary sources, all constructs, indicators, and inter-relationships reported in

Sections 5–7 represent a synthesis of published literature rather than the outcome of primary statistical analysis.

3.6. Future Scope

The suggested methodology should be empirically tested in further studies using primary data gathered from structured questionnaires given to salaried women in various industries, income brackets, and geographical areas. The proposed correlations between independent, mediating, and outcome factors might be statistically validated using structural equation modelling (SEM). (Hair et al., 2022). Comparative studies across different demographic segments, age groups, urban versus rural, and public versus private sector employees would further strengthen the generalisability of the framework.

4. Results of the Conceptual Synthesis

As this study is conceptual and descriptive in nature, drawing entirely on secondary literature and institutional data, the “results” reported here are the outcomes of the thematic and secondary-data synthesis (Tables 1–4; Figure 1) rather than results of primary statistical testing. Two visual summaries a thematic-frequency chart and a source-composition chart are presented below to make these synthesis outcomes easier to interpret.

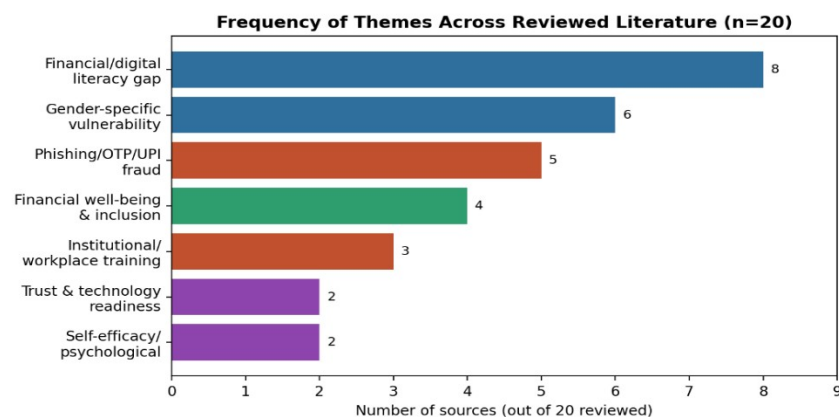


Fig 5 Frequency of Themes Across Reviewed Literature (n = 20)

Source: Authors' own thematic synthesis, derived from Table 2. The conceptual content was generated using ChatGPT 5.5, and the visualisation was created using Napkin AI.

Key results emerging from the synthesis are summarised below:

- The financial/digital literacy gap (8/20 sources, 40%) and gender-specific vulnerability (6/20, 30%) are the two most recurring themes, together accounting for 70% of the reviewed literature, confirming that awareness deficits and gendered risk exposure are the dominant concerns in existing research.
- Fraud-specific literature (phishing, OTP fraud, UPI-related fraud) constitutes 5/20 sources (25%), reflecting a growing institutional and regulatory concern that is not yet matched by an equivalent volume of academic, women-focused research.
- Psychological mediating themes trust in digital platforms and self-efficacy are the least represented, at 2/20 sources (10%) each. This is the clearest empirical gap identified by the synthesis and is the primary justification for the mediating variables proposed in Section 4.

- The secondary trend-data analysis (Table 3, Figure 1) shows an 85% year-on-year increase in reported UPI fraud cases between FY 2022–23 and FY 2023–24, with the amount involved nearly doubling, evidence that the pace of digital-payment fraud is outstripping the pace of user awareness.
- The proposed framework (Section 4) synthesises 11 constructs in total 4 independent, 3 mediating, 1 composite dependent, and 3 outcome variables built from the patterns identified across the 20 reviewed sources and the 4 theoretical models summarised in Table 5.

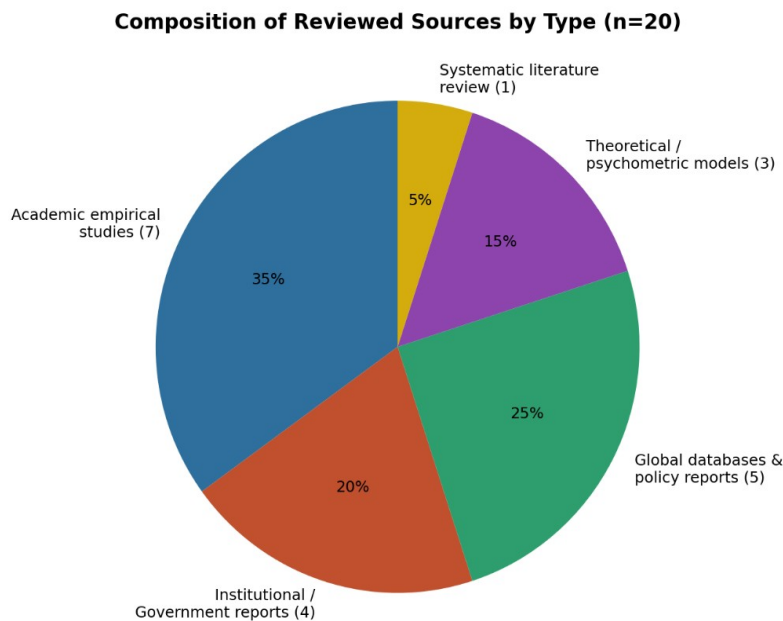


Fig 6. Composition of Reviewed Sources by Type (n = 20)

Source: Authors' own classification of the sources listed in Table 1. The conceptual content was generated using ChatGPT 5.5, and the visualisation was created using Napkin AI.

The source-composition chart shows that the review draws on a balanced mix of academic empirical studies (35%), institutional/government reports (20%), global databases and policy reports (25%), established theoretical/psychometric models (15%), and one systematic literature review (5%). This spread supports the conceptual, multi-source triangulation approach adopted in this paper (Section 9).

5. Discussion

The synthesis results discussed above carry several interpretive implications for understanding digital financial security awareness among salaried women.

5.1. Awareness Deficits Remain the Central Concern

The dominance of the financial/digital literacy theme (40% of reviewed sources) is consistent with the OECD/INFE (2020) Knowledge-Attitude-Behaviour framework and with Kaur and Arora (2021), both of which treat literacy gaps as the starting point for any awareness intervention. This reinforces the positioning of Digital Literacy Level and Demographic Factors as independent variables in the proposed framework (Section 4.2), since the literature consistently treats them as antecedents rather than outcomes.

5.2. Gendered Risk Exposure is Well Documented but Under-theorised

Gender-specific vulnerability is the second-most recurring theme (30%), corroborated by hard administrative data NCRB (2023) and the 85% year-on-year rise in UPI fraud (Ministry of Finance, 2024). However, most sources reporting this vulnerability (RBI, NPCI, CERT-In, NCRB) are descriptive, incidence-based reports rather than explanatory studies. This gap between documented incidence and explanatory theory is precisely what the proposed conceptual framework attempts to close by introducing risk perception, trust, and self-efficacy as explicit mediating mechanisms (Section 4.3).

5.3. Psychological Mediators Are the Clearest Research Gap

Trust and self-efficacy each appear in only 2 of the 20 reviewed sources, and almost exclusively in theoretical/psychometric work (Rogers, 1975; Parasuraman & Colby, 2015) rather than in women-focused or India-specific empirical studies. This scarcity directly supports the paper's central contribution: existing literature explains *that* awareness gaps and vulnerability exist, but rarely explains *how* antecedents translate into safe behaviour. The mediating layer proposed in this framework is designed to fill exactly this explanatory gap.

5.4. Institutional Data Confirms Urgency, but Not Behavioural Insight

Institutional and government sources (RBI, NPCI, CERT-In, NCRB — 20% of reviewed sources) consistently confirm that digital fraud is rising faster than user protection. This validates the practical urgency of the topic (Section 2) but, as these sources are incidence- and enforcement-focused rather than behavioural, they cannot by themselves explain why salaried women remain disproportionately vulnerable — reinforcing the need for the psychology-informed academic lens this paper adopts (Rogers, 1975; Parsons et al., 2017).

5.5. Balanced Source Composition Strengthens the Conceptual Base

The near-even split across academic, institutional, global-database, and theoretical sources (Figure 5) suggests the proposed framework is not built on a narrow evidentiary base. At the same time, since all synthesis in this paper is qualitative and secondary in nature, these results should be read as directional patterns rather than statistically validated findings, a limitation already noted in Section 10 and revisited in Section 12.

5.6. Limitations of the Study

- The framework is conceptual in nature and has been developed entirely from secondary data and literature synthesis; it has not yet been empirically tested or statistically validated.
- The relationships proposed between constructs are based on theoretical reasoning and prior secondary studies in related domains (Rogers, 1975; Parasuraman & Colby, 2015; Parsons et al., 2017), and actual relationships may vary across regions and demographic groups.
- Being based entirely on secondary sources, the study is subject to the limitations, scope, and currency of the reports and literature reviewed (RBI, 2023–2025; NPCI, 2023–2025).
- The thematic content analysis (Table 2) and fraud-trend analysis (Table 3, Figure 1) are both derived from secondary sources and are illustrative of broader patterns rather than a statistically validated or exhaustive analysis; the FY 2024–25 figures are provisional and cover only part of the financial year.

6. Conclusion

As digital financial transactions become deeply embedded in everyday life, ensuring adequate digital financial security awareness among salaried women is both a practical necessity and a matter of financial inclusion equity [18]. Through the mediating mechanisms of risk perception, trust, and self-efficacy, this research has provided an integrated conceptual framework based solely on secondary data that connects digital financial security awareness to demographic, technological, and social antecedents. [12], [14], [16]. ultimately leading to safer financial behaviour and improved financial well-being.

Despite being conceptual in nature, the framework provides an organised basis for further empirical studies as well as for the creation of more successful, focused awareness campaigns by employers, legislators, and financial institutions.[21], [22], [24]. The framework identifies risk perception, trust, and self-efficacy as mediating variables; digital literacy, social influence, institutional training, and self-efficacy as significant independent variables; and safe digital financial behaviour, decreased fraud vulnerability, and improved financial well-being as outcome variables. This paper includes the theoretical contributions, managerial and policy implications, and future directions for empirical validation of the proposed paradigm.[21], [22]. [23].

Acknowledgements

The authors express their sincere gratitude to Dr. Dineshkumar R. Chavda, Research Guide, for his valuable guidance, continuous encouragement, and constructive support throughout this study. The author also wishes to express her deepest gratitude to her beloved parents, Mr. Dineshbhai Vikrambhai Suva and Mrs. Manjuben Dineshbhai Suva, for their unconditional love, constant support, inspiration, and encouragement, which have been the greatest source of strength throughout her academic journey. Finally, the author sincerely thanks the Department of Commerce and Management, Bhakta Kavi Narsinh Mehta University, Junagadh, for providing a supportive academic environment for completing this study. The author declares that no external financial support or research funding was received for this study.

Funding

This research received no external funding.

Conflict of Interest

The Authors declare that they have no conflict of interest.

Data Availability Statement

The data supporting the findings of this study are derived from publicly available secondary sources, including peer-reviewed journal articles, government reports, institutional publications, and other publicly accessible documents cited in the reference list.

AI Usage Disclosure

The authors used ChatGPT (OpenAI), Grammarly, and DeepL Write only for language editing, grammar correction, and improving the clarity of the manuscript. All conceptualisation, literature review, thematic

analysis, figures, tables, interpretation, and final content were independently developed, verified, and approved by the authors, who take full responsibility for the manuscript.

Author Contributions

Conceptualisation: Harshitaben Dineshbhai Suva and Dr Dineshkumar R. Chavda;

Methodology: Harshitaben Dineshbhai Suva; Formal analysis: Harshitaben Dineshbhai Suva;

Investigation: Harshitaben Dineshbhai Suva;

Writing – original draft: Harshitaben Dineshbhai Suva;

Writing – review and editing: Dr. Dineshkumar R. Chavda.

All authors have read and agreed to the published version of the manuscript

References

- [1] Agrawal, V., & Agarwal, M. (2023). Evaluating Financial Literacy Among Working Women in Pune: A Gender-Sensitive Approach. *Innovation-Driven Business and Sustainability in the Tropics*, 419–430. https://doi.org/10.1007/978-981-99-2909-2_24
- [2] Ali, U., Fatima, H., Rehman, J., & Baloch, S. (2024). Evaluating the Impact of Financial Literacy on Investment Decisions: A Case Study of Balochistan, Pakistan. *Journal of Entrepreneurship, Management, and Innovation*, 6(1), 35–56.
- [3] CERT-In (Indian Computer Emergency Response Team). (2023–2025). *Cybersecurity bulletins and advisories on digital payment fraud*. Ministry of Electronics and Information Technology, Government of India. <https://www.cert-in.org.in/>
- [4] Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). *A primer on partial least squares structural equation modelling (PLS-SEM)* (3rd ed.). Sage. https://www.google.com/books/edition/A_Primer_on_Partial_Least_Squares_Structural_Equation_Modelling/wSbrEAAAQBAJ
- [5] Jainy Rahulkumar, S., & Patel, K. (2025). Assessing the financial well-being of working women in Gujarat: The role of financial literacy and investment decisions. *Advances in Consumer Research*, 2(4), 5511–5520. <https://acr-journal.com/>
- [6] Kaur, H., & Arora, S. (2021). Digital banking awareness among working women: An empirical study. *Journal of Financial Literacy Studies*, 8(2), 45–58.
- [7] Klapper, L., & Arora, T. (2022). *Improving women's access to credit in India*. World Bank. <https://blogs.worldbank.org>
- [8] Kulkarni, L., & Ghosh, A. (2021). Gender disparity in the digitalisation of financial services: Challenges and promises for women's financial inclusion in India. *Gender, Technology and Development*, 25(2), 233–250. <https://doi.org/10.1080/09718524.2021.1911022>
- [9] Kumari, P., & Devi, R. (2022). Gender differentials in vulnerability to cyber-financial fraud. *International Journal of Cyber Studies*, 5(1), 22–34.
- [10] Kumar, S. (2023). *Financial inclusion of women: Current evidence from India*. Observer Research Foundation. <https://www.orfonline.org>
- [11] Ministry of Finance, Government of India. (2023). *Pradhan Mantri Jan Dhan Yojana (PMJDY) progress report*. <https://pmjdy.gov.in>
- [12] Ministry of Finance, Government of India. (2024, November 25). *Response to unstarred question on domestic UPI-related frauds*. Lok Sabha, Winter Session. <https://www.medianama.com/2024/11/223-upi-fraud-up-85-per-cent-fy2023-24-finance-ministry-data/>
- [13] National Crime Records Bureau. (2023). *Crime in India: Cyber crime statistics report*. Ministry of Home Affairs, Government of India. <https://ncrb.gov.in/>

- [14] National Payments Corporation of India. (2023–2025). *UPI transaction and fraud trend reports*. <https://www.npci.org.in/>
- [15] OECD/INFE. (2020). *International survey of adult financial literacy*. Organisation for Economic Co-operation and Development. https://www.oecd.org/en/publications/2020/06/oecd-infe-2020-international-survey-of-adult-financial-literacy_bbad9b27.html
- [16] Parasuraman, A., & Colby, C. L. (2015). An updated and streamlined technology readiness index: TRI 2.0. *Journal of Service Research*, 18(1), 59–74. <https://doi.org/10.1177/1094670514539730>
- [17] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42, 165–176. <https://doi.org/10.1016/j.cose.2017.01.004>
- [18] Patel, P., Kolte, H., & Satish, R. (2025). Financial literacy and its determinants among tribal women: Evidence from Raigarh District, Chhattisgarh, India. *Advancement in Management and Technology*, 6(2), 8–16. <https://doi.org/10.46977/amt.2025.v06i02.002>
- [19] Reserve Bank of India. (2023–2025). *Reports on digital payment security and financial literacy*. RBI Publications. <https://www.rbi.org.in/>
- [20] Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93–114. <https://doi.org/10.1080/00223980.1975.9915803>
- [21] World Bank. (2021). *The Global Findex Database: Financial inclusion, digital payments, and resilience*. <https://www.worldbank.org/en/publication/globalfindex>
- [22] Yohana, E., & Masdupi, E. (2023). The Influence of Financial Knowledge on Tax Literacy with Individual Financial Management Behaviour as a Mediation Variable and Living Cost as a Control Variable in Generation “Z” in Padang City. *Advances in Economics, Business and Management Research*, 250, 57–73. https://doi.org/10.2991/978-94-6463-158-6_6
- [23] Zainuddin, A., Aziz, F. M. M., Harith, N. H. M., Rahim, M. A., & Yusoff, B. (2024). Financial Literacy in Improving Financial Well-Being Among Female Civil Servants: A Study in Putrajaya. *Pakistan Journal of Life and Social Sciences*, 22(2), 140–155. <https://doi.org/10.57239/PJLSS-2024-22.2.0011>
- [24] Zainuddin, A., Rahim, M. A., Hafizah Harith, N. M., Najiha Nizam, S. S., Technology MARA, U., & Alam, S. (2025). Domains of Financial Literacy Among Women in Public Sector: A Systematic Literature Review. *Pegem Journal of Education and Instruction*, 15(2), 105–115. <https://doi.org/10.47750/pegegog.15.10.11>