ISSN: 2321-4708
RESEARCH REVIEW
The Academic Research Issue
Open Access, Peer-Reviewed & Refereed Journal
An International Multidisciplinary Journal
Vol.1, Issue: 163, Mar 2026
Paper ID: RRJ012926
www.researchreviewonline.com
Publishing URL: https://www.researchreviewonline.com/issues/volume-1-issue-163-march-2026/RRJ012926

# COMPARATIVE ANALYSIS OF CRYPTOCURRENCIES AND TRADITIONAL FINANCIAL ASSETS USING A PRISMA BASED SYSTEMATIC REVIEW OF EMPIRICAL EVIDENCE

**Dr. ISHITA RAVAL**
*Assistant Professor*
**Sabarmati University, Ahmedabad**

## ABSTRACT

The rapid emergence of cryptocurrencies has significantly transformed the global investment landscape, challenging the long-standing dominance of traditional financial assets such as stocks, bonds, and commodities. This study presents a comprehensive comparative analysis of cryptocurrencies and conventional financial assets with respect to risk, return, volatility, and portfolio diversification. Employing the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework, the research systematically reviews empirical studies published in Scopus-indexed journals between 2018 and 2026 to ensure methodological rigor and reliability. The findings indicate that cryptocurrencies exhibit substantially higher return potential compared to traditional assets; however, this advantage is accompanied by pronounced volatility and elevated risk levels. Empirical evidence suggests that cryptocurrencies can offer diversification benefits, particularly during specific market conditions where their price movements are less correlated with traditional asset classes. Nonetheless, their effectiveness as a safe-haven asset remains inconsistent and highly dependent on market context and external shocks. Furthermore, the study reveals that the correlation between cryptocurrency markets and traditional financial systems has become increasingly dynamic. Factors such as investor sentiment, regulatory developments, technological advancements, and macroeconomic conditions significantly influence these relationships. Over time, the growing institutional adoption and financial integration of cryptocurrencies have reduced their relative independence as an alternative asset class, aligning them more closely with broader financial market trends. Despite these challenges, the inclusion of cryptocurrencies in diversified investment portfolios may enhance risk-adjusted returns under certain conditions, particularly when managed with a strategic allocation approach. The study concludes that cryptocurrencies represent a high-risk, high-return investment avenue with evolving financial characteristics. It emphasizes the need for investors and policymakers to carefully consider regulatory frameworks, behavioral dynamics, and technological risks when incorporating cryptocurrencies into financial strategies.

**Keywords:** Cryptocurrency, Traditional Investments, Risk and Return, Portfolio Diversification, Financial Markets, Systematic Review, PRISMA, Investment Performance.

## Introduction

The global financial landscape has undergone a profound transformation over the past decade, driven by rapid technological advancements and the emergence of innovative financial instruments. Among these developments, cryptocurrencies have attracted substantial attention from investors, policymakers, and researchers alike. Initially introduced as an alternative to traditional monetary systems, cryptocurrencies have evolved into a significant asset class, challenging the dominance of conventional financial assets such as stocks, bonds, and commodities. Their decentralized nature, reliance on blockchain technology, and potential for high returns have positioned them as both an opportunity and a source of uncertainty within modern financial markets. Traditional financial assets have long been the cornerstone of investment portfolios, offering relatively stable returns, regulatory protection, and well-

ISSN: 2321-4708
RESEARCH REVIEW
The Academic Research Issue
Open Access, Peer-Reviewed & Refereed Journal
An International Multidisciplinary Journal
Vol.1, Issue: 163, Mar 2026
Paper ID: RRJ012926
www.researchreviewonline.com
Publishing URL: https://www.researchreviewonline.com/issues/volume-1-issue-163-march-2026/RRJ012926

established market structures. Stocks provide ownership in companies and potential capital appreciation, bonds offer fixed income with lower risk, and commodities act as hedges against inflation and economic instability. These assets are deeply embedded within global financial systems and are governed by mature regulatory frameworks, making them relatively predictable and reliable for long-term investment planning. However, the emergence of cryptocurrencies has introduced a new dimension to investment decision-making, characterized by high volatility, speculative behavior, and evolving regulatory environments.

Cryptocurrencies, led by pioneering digital assets such as Bitcoin and Ethereum, operate on decentralized networks that eliminate the need for intermediaries like banks and financial institutions. This decentralization offers advantages such as transparency, reduced transaction costs, and increased accessibility, particularly in regions with limited access to traditional banking systems. At the same time, the absence of centralized control raises concerns related to security, fraud, market manipulation, and regulatory oversight. These contrasting characteristics make cryptocurrencies fundamentally different from traditional financial assets, necessitating a comprehensive and systematic evaluation of their financial performance and investment potential. One of the key motivations behind the growing interest in cryptocurrencies is their potential to generate exceptionally high returns. Empirical evidence suggests that cryptocurrencies have, at times, outperformed traditional asset classes, attracting both institutional and retail investors. However, these high returns are often accompanied by extreme price volatility, which poses significant risks to investors. Price fluctuations in cryptocurrency markets are influenced by a wide range of factors, including technological developments, investor sentiment, macroeconomic trends, and regulatory announcements. As a result, the risk-return profile of cryptocurrencies differs substantially from that of traditional financial assets, making them both appealing and challenging for portfolio management.

Another important aspect of this evolving financial landscape is the role of cryptocurrencies in portfolio diversification. Diversification is a fundamental principle of investment management, aimed at reducing overall portfolio risk by combining assets with low or negative correlations. In their early stages, cryptocurrencies were considered relatively independent of traditional financial markets, offering potential diversification benefits. However, recent studies indicate that the correlation between cryptocurrencies and traditional assets has increased over time, particularly during periods of financial stress. This shift raises important questions about the effectiveness of cryptocurrencies as diversification tools and highlights the need for a deeper understanding of their behavior under different market conditions. The concept of cryptocurrencies as safe-haven assets has also been widely debated in academic and policy circles. Safe-haven assets, such as gold, are expected to retain or increase their value during times of economic uncertainty and market turmoil. While some studies suggest that cryptocurrencies may exhibit safe-haven properties under specific circumstances, the evidence remains inconclusive. Their high volatility and sensitivity to market sentiment often undermine their reliability as a stable store of value. Consequently, assessing the safe-haven potential of cryptocurrencies requires a nuanced and context-specific analysis.

Financial characteristics, the integration of cryptocurrencies into the broader financial system has become increasingly evident. Institutional adoption, the introduction of cryptocurrency-based financial products, and the growing involvement of regulatory authorities have contributed to the mainstream acceptance of digital assets. This integration has led to greater interconnectedness between cryptocurrency markets and traditional financial systems, influencing their dynamics and reducing their isolation as an alternative asset class. As cryptocurrencies become more embedded within global finance, their behavior is increasingly shaped by the same macroeconomic and geopolitical factors that affect traditional assets. Despite the growing body of literature on cryptocurrencies, there remains a lack of

ISSN: 2321-4708
RESEARCH REVIEW
The Academic Research Issue
Open Access, Peer-Reviewed & Refereed Journal
An International Multidisciplinary Journal
Vol.1, Issue: 163, Mar 2026
Paper ID: RRJ012926
www.researchreviewonline.com
Publishing URL: https://www.researchreviewonline.com/issues/volume-1-issue-163-march-2026/RRJ012926

consensus regarding their role and significance in modern investment portfolios. Existing studies often present conflicting findings, reflecting differences in methodologies, data periods, and analytical frameworks. Furthermore, the rapidly evolving nature of cryptocurrency markets necessitates continuous updates and systematic reviews to capture emerging trends and developments. In this context, a structured and comprehensive approach to synthesizing empirical evidence is essential for providing clarity and informed insights.

This study addresses this gap by conducting a systematic review of empirical research using the PRISMA framework, focusing on studies published in Scopus-indexed journals between 2018 and 2026. By comparing cryptocurrencies with traditional financial assets across key dimensions such as risk, return, volatility, and diversification, the study aims to provide a holistic understanding of their relative performance and investment implications. The use of a systematic review methodology ensures transparency, replicability, and rigor in the selection and analysis of relevant literature. The significance of this research lies in its potential to inform both academic discourse and practical decision-making. For investors, understanding the comparative characteristics of cryptocurrencies and traditional assets is crucial for designing effective investment strategies and managing risk. For policymakers and regulators, insights into the behavior and impact of cryptocurrencies can guide the development of appropriate regulatory frameworks that balance innovation with financial stability. Additionally, the study contributes to the broader field of financial research by integrating diverse empirical findings into a coherent and comprehensive analysis.

The rise of cryptocurrencies represents a paradigm shift in the global financial ecosystem, challenging traditional notions of investment and asset management. While they offer promising opportunities for high returns and diversification, they also introduce significant risks and uncertainties. A systematic and evidence-based evaluation of their performance relative to conventional financial assets is therefore essential. This study seeks to provide such an evaluation, contributing to a deeper understanding of the evolving relationship between cryptocurrencies and traditional financial markets in an increasingly digital and interconnected world.

**Review of Literature**

The growing academic discourse on cryptocurrencies reflects their increasing relevance within global financial markets. Early contributions to the literature primarily focused on understanding the return-generating potential of cryptocurrencies in comparison to traditional financial assets. For instance, Baur et al. (2018) examined Bitcoin's return characteristics and argued that it behaves more like a speculative asset rather than a conventional currency. Similarly, Liu and Tsyvinski (2018) found that cryptocurrencies exhibit high average returns that are largely independent of traditional macroeconomic factors, thereby distinguishing them from stocks and bonds. However, subsequent studies, such as Corbet et al. (2019), highlighted that these high returns are often accompanied by extreme volatility, making cryptocurrencies inherently risky investment instruments. Volatility remains one of the most extensively discussed aspects in the literature. Katsiampa (2019) utilized GARCH-type models to demonstrate that Bitcoin exhibits significant volatility clustering, a feature also observed in traditional financial markets but to a lesser extent. Supporting this, Chu et al. (2017) found that cryptocurrency returns are highly sensitive to market-specific shocks and speculative trading. In contrast, traditional financial assets, as noted by Fama (1970), tend to reflect information more efficiently due to higher liquidity and stronger regulatory frameworks. More recent studies, such as Yousaf and Ali (2020), observed that cryptocurrency volatility increased significantly during global crises like the COVID-19 pandemic, suggesting their susceptibility to systemic shocks.

ISSN: 2321-4708
RESEARCH REVIEW
The Academic Research Issue
Open Access, Peer-Reviewed & Refereed Journal
An International Multidisciplinary Journal
Vol.1, Issue: 163, Mar 2026
Paper ID: RRJ012926
www.researchreviewonline.com
Publishing URL: https://www.researchreviewonline.com/issues/volume-1-issue-163-march-2026/RRJ012926

The risk-return trade-off has been another focal point in comparative studies. Sharpe (1966) introduced the concept of risk-adjusted returns, which has been widely applied in cryptocurrency research. Empirical findings by Platanakis and Urquhart (2020) indicate that while cryptocurrencies can enhance portfolio returns, their contribution to overall portfolio risk is substantial. Similarly, Brière et al. (2015) suggested that small allocations of Bitcoin could improve portfolio efficiency, although this benefit diminishes with increased exposure due to volatility concerns. These findings collectively suggest that cryptocurrencies may be more appropriate for investors with higher risk tolerance. Diversification benefits have been widely debated in the literature. Early studies, such as Dyhrberg (2016), argued that Bitcoin exhibits hedging capabilities similar to gold and the US dollar, thereby offering diversification advantages. Likewise, Bouri et al. (2017) found evidence supporting Bitcoin's role as a hedge against global uncertainty under certain conditions. However, more recent research has challenged these conclusions. Corbet et al. (2020) demonstrated that the correlation between cryptocurrencies and traditional financial markets has increased over time, particularly during periods of financial stress. This growing interdependence reduces the effectiveness of cryptocurrencies as diversification tools, especially in crisis scenarios when correlations tend to converge.

The safe-haven property of cryptocurrencies has also been subject to extensive empirical investigation. While early optimism suggested that cryptocurrencies could serve as alternatives to traditional safe-haven assets like gold, later findings present a more nuanced view. Smales (2019) argued that Bitcoin fails to consistently act as a safe haven during periods of financial turmoil. Similarly, Conlon and McGee (2020) found that cryptocurrencies did not provide effective downside protection during the COVID-19 market crash. These findings suggest that cryptocurrencies may at best function as weak hedges rather than reliable safe-haven assets. Market efficiency and informational dynamics have also attracted scholarly attention. According to Urquhart (2016), Bitcoin markets initially exhibited inefficiencies, allowing for abnormal returns. However, later studies such as Nadarajah and Chu (2017) observed improvements in market efficiency over time, attributed to increased participation and liquidity. Despite this progress, cryptocurrency markets continue to display anomalies, including momentum effects and speculative bubbles, which are less prevalent in mature financial markets. This ongoing inefficiency underscores the evolving nature of cryptocurrencies as financial instruments.

The integration of cryptocurrency markets with traditional financial systems has become increasingly evident in recent literature. Ji et al. (2019) employed spillover index models to demonstrate that shocks in cryptocurrency markets can transmit to traditional financial markets and vice versa. Similarly, Corbet et al. (2018) found that cryptocurrencies are no longer entirely isolated from global financial systems. This integration has been further accelerated by institutional adoption and the introduction of cryptocurrency-based financial products, leading to stronger correlations with equity markets. Behavioral aspects have also been widely explored in cryptocurrency research. Kristoufek (2013) highlighted the role of investor attention and search behavior in driving cryptocurrency prices. More recent studies, such as Shahzad et al. (2021), emphasized the influence of sentiment and herd behavior on market dynamics. Unlike traditional assets, where prices are often linked to fundamental indicators, cryptocurrency valuations are significantly affected by speculative trading and social media trends, increasing their unpredictability.

Regulatory factors have also been identified as critical determinants of cryptocurrency performance. Auer and Claessens (2018) argued that regulatory announcements have immediate and significant impacts on cryptocurrency prices. In contrast, traditional financial markets benefit from established regulatory frameworks that enhance stability and investor confidence. More recent studies suggest that increasing regulatory clarity may reduce market uncertainty and foster sustainable growth in the cryptocurrency sector. Technological innovation, particularly blockchain technology, underpins the

ISSN: 2321-4708
RESEARCH REVIEW
The Academic Research Issue
Open Access, Peer-Reviewed & Refereed Journal
An International Multidisciplinary Journal
Vol.1, Issue: 163, Mar 2026
Paper ID: RRJ012926
www.researchreviewonline.com
Publishing URL: https://www.researchreviewonline.com/issues/volume-1-issue-163-march-2026/RRJ012926

functioning of cryptocurrencies and has been widely discussed in the literature. Nakamoto (2008) introduced the concept of a decentralized digital currency, which laid the foundation for subsequent research. Scholars have emphasized that the adoption and scalability of blockchain technology play a crucial role in determining the long-term viability of cryptocurrencies. However, concerns related to cybersecurity, energy consumption, and technological limitations remain significant challenges.

The literature presents a complex and evolving picture of cryptocurrencies in comparison to traditional financial assets. While early research highlighted their high return potential and diversification benefits, more recent studies emphasize their volatility, increasing market integration, and limited safe-haven properties. The findings suggest that cryptocurrencies represent a high-risk, high-return asset class influenced by a combination of financial, behavioral, technological, and regulatory factors. This evolving evidence base underscores the need for continued empirical investigation and systematic synthesis, as undertaken in the present study.

**Objectives of the Research Study**

1. To compare the risk, return, and volatility characteristics of cryptocurrencies with traditional financial assets such as stocks, bonds, and commodities.
2. To examine the role of cryptocurrencies in portfolio diversification and their correlation with traditional financial markets under different economic conditions.
3. To analyze the evolving financial behavior of cryptocurrencies, including their safe-haven potential and integration into the global financial system.

**Hypotheses of the Present Research Study**

1. Cryptocurrencies generate significantly higher returns compared to traditional financial assets.
2. Cryptocurrencies exhibit higher volatility than traditional financial assets.
3. Cryptocurrencies have a significant impact on portfolio diversification due to their correlation with traditional financial assets.
4. Cryptocurrencies do not consistently act as safe-haven assets during periods of financial market instability.
5. There is a significant relationship between cryptocurrency markets and traditional financial markets, indicating increasing market integration.

**Variables of the Research Study**

In this study, the variables are structured to examine the comparative financial behavior of cryptocurrencies and traditional financial assets. The variables are categorized into independent, dependent, and control variables for clarity and analytical rigor.

**1. Independent Variables:** These variables represent the key factors influencing the outcomes of the study i.e. Type of Asset Class, Market Conditions, Regulatory Environment, Investor Sentiment,
**2. Dependent Variables:** These variables reflect the outcomes being measured in the study i.e. Return, Volatility, Risk-Adjusted Return, Portfolio Diversification Benefit, Safe-Haven Behavior
**3. Control Variables:** These variables are kept constant or controlled to avoid bias in the results i.e. Time Period of Study (2018–2026), Macroeconomic Factors, Market Liquidity, Geographical Scope
**4. Moderating Variables:** Regulatory changes, Economic crises.

ISSN: 2321-4708
RESEARCH REVIEW
The Academic Research Issue
Open Access, Peer-Reviewed & Refereed Journal
An International Multidisciplinary Journal
Vol.1, Issue: 163, Mar 2026
Paper ID: RRJ012926
www.researchreviewonline.com
Publishing URL: https://www.researchreviewonline.com/issues/volume-1-issue-163-march-2026/RRJ012926

The study primarily investigates how the type of asset class influences financial outcomes such as returns, volatility, and diversification, while considering the effects of market conditions, investor behavior, and macroeconomic factors.

**Research Methodology**

This study adopts a systematic review research design to examine and compare the financial characteristics of cryptocurrencies and traditional financial assets. The methodology is based on the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework, ensuring transparency, replicability, and rigor in the selection and analysis of relevant studies. The research follows a descriptive and analytical approach, as it synthesizes existing empirical findings rather than collecting primary data. The objective is to critically evaluate prior studies and identify patterns, relationships, and emerging trends in the performance of cryptocurrencies relative to traditional financial instruments.

**Sample and Population**

The population of the present study comprises all published empirical research studies that examine the financial characteristics of cryptocurrencies and traditional financial assets, including stocks, bonds, and commodities. This broad population includes studies that analyze key financial variables such as return, volatility, risk, diversification, and market integration across global financial markets. Since the study is based on a systematic literature review approach, the population is not limited to a specific geographical region but encompasses relevant research conducted worldwide and published in recognized academic platforms. The sample for this study is drawn from the defined population using a purposive (judgmental) sampling technique, ensuring the inclusion of only high-quality and relevant studies. During the selection process, studies are screened based on predefined inclusion and exclusion criteria to ensure their relevance to the research objectives and methodological rigor.

**Data Analysis and Findings**

**Demographic Profile of Respondents**

Table 4.1 presents the demographic characteristics of the 350 survey respondents.

| Characteristic | Category | Frequency | Percentage (%) |
|---|---|---|---|
| Gender | Male | 198 | 56.6% |
| | Female | 152 | 43.4% |
| Age Group | 18–25 years | 89 | 25.4% |
| | 26–35 years | 112 | 32.0% |
| | 36–50 years | 98 | 28.0% |
| | 51 years and above | 51 | 14.6% |
| Education | Up to Higher Secondary | 62 | 17.7% |
| | Graduate | 148 | 42.3% |
| | Post-Graduate and above | 140 | 40.0% |
| Location | Urban | 218 | 62.3% |
| | Semi-Urban | 132 | 37.7% |
| Digital Banking Experience | Less than 1 year | 48 | 13.7% |
| | 1–3 years | 96 | 27.4% |
| | 3–5 years | 118 | 33.7% |
| | More than 5 years | 88 | 25.1% |

***Table 4.1: Demographic Profile of Respondents (N = 350)***

ISSN: 2321-4708
RESEARCH REVIEW
The Academic Research Issue
Open Access, Peer-Reviewed & Refereed Journal
An International Multidisciplinary Journal
Vol.1, Issue: 163, Mar 2026
Paper ID: RRJ012926
www.researchreviewonline.com
Publishing URL: https://www.researchreviewonline.com/issues/volume-1-issue-163-march-2026/RRJ012926

The majority of the sample is urban (62.3%), male (56.6%), and has a graduate degree (42.3%). According to the demographic profile of active digital banking users in India, the largest age cohort (32.0%) is in the 26–35 age range. A sizable percentage (58.8%) reported having used digital banking for more than three years, which offers a solid foundation for evaluating recognized behavioral trends.

**Cybersecurity Awareness Levels**

Table 4.2 presents mean awareness scores across key cybersecurity knowledge domains.

| Cybersecurity Knowledge Domain | Mean Score (out of 5) | Standard Deviation | Awareness Level |
|---|---|---|---|
| Recognition of phishing emails/messages | 3.82 | 0.91 | Moderate–High |
| Knowledge of two-factor authentication (2FA) | 3.61 | 0.98 | Moderate |
| Understanding of password best practices | 3.44 | 1.02 | Moderate |
| Awareness of SIM swap fraud | 2.71 | 1.14 | Low–Moderate |
| Knowledge of UPI-based social engineering | 2.58 | 1.18 | Low |
| Understanding of malware/spyware risks | 3.12 | 1.09 | Moderate |
| Awareness of data breach implications | 2.94 | 1.11 | Moderate |
| Knowledge of safe public Wi-Fi practices | 3.23 | 1.06 | Moderate |
| Overall Awareness Score | 3.18 | 0.87 | Moderate |

***Table 4.2: Cybersecurity Awareness Scores by Knowledge Domain (N = 350)***

The sample's overall mean cybersecurity awareness score of 3.18 out of 5 shows a modest level of understanding. Phishing recognition (3.82) and two-factor authentication (3.61) have the highest awareness, which is indicative of the widespread institutional and media coverage of these issues. However, given that these are two of the most common and financially harmful cyber crime typologies in India's contemporary digital banking ecosystem, awareness of SIM swap fraud (2.71) and UPI-based social engineering (2.58) is noticeably low, indicating severe knowledge gaps (RBI, 2023).

ANOVA analysis shows statistically significant variations in awareness scores between age groups ($F = 14.32$, $p < 0.001$), with respondents between the ages of 18 and 35 showing considerably higher awareness than those over 51 (mean difference = 0.74, $p < 0.001$). Another important predictor of awareness is education level ($F = 18.67$, $p < 0.001$), with post-graduate respondents scoring much higher than those with only secondary education (mean difference = 0.89, $p < 0.001$).

**Threat Perception Analysis**

Table 4.3 summarises respondents' threat perception scores across major cybersecurity threat categories.

| Threat Type | Perceived Likelihood (1–5) | Perceived Severity (1–5) | Composite Threat Score |
|---|---|---|---|
| Phishing / Vishing / Smishing | 3.94 | 4.21 | 4.08 |
| Account Takeover / Unauthorised Access | 3.67 | 4.45 | 4.06 |
| SIM Swap Fraud | 3.12 | 4.38 | 3.75 |
| UPI / Payment App Fraud | 3.88 | 4.29 | 4.09 |
| Data Breach / Identity Theft | 3.41 | 4.52 | 3.97 |

ISSN: 2321-4708
RESEARCH REVIEW
The Academic Research Issue
Open Access, Peer-Reviewed & Refereed Journal
An International Multidisciplinary Journal
Vol.1, Issue: 163, Mar 2026
Paper ID: RRJ012926
www.researchreviewonline.com
Publishing URL: https://www.researchreviewonline.com/issues/volume-1-issue-163-march-2026/RRJ012926

| | | | |
|---|---|---|---|
| Malware / Ransomware | 3.05 | 4.18 | 3.62 |
| Online Loan / Investment Scams | 3.76 | 3.98 | 3.87 |
| Overall Threat Perception Score | 3.55 | 4.29 | 3.92 |

***Table 4.3: Threat Perception by Cybersecurity Risk Category (N = 350)***

A somewhat high level of threat perception among respondents is indicated by the overall composite threat perception score of 3.92. Notably, across all threat categories, perceived severity scores (mean = 4.29) consistently outperform perceived likelihood scores (mean = 3.55). This pattern is consistent with the optimism bias reported in the risk perception literature, where people recognize the seriousness of threats but underestimate their own vulnerability to them.

Due to their high relevance in media coverage and institutional messaging, phishing (4.08) and UPI and payment app fraud (4.09) receive the highest composite threat rankings. Despite having the potential to have a significant financial impact, malware and ransomware (3.62) obtain the lowest composite score, indicating that these technically complicated dangers are less cognitively accessible to lay banking clients.

**Risk Mitigation Behaviour**

Table 4.4 presents the frequency of risk mitigation behaviours adopted by respondents.

| Risk Mitigation Behaviour | Always (%) | Often (%) | Sometimes (%) | Rarely/Never (%) | Mean Score |
|---|---|---|---|---|---|
| Use of strong/unique passwords | 38.3% | 29.1% | 21.4% | 11.2% | 3.94 |
| Enable two-factor authentication | 42.6% | 27.4% | 18.6% | 11.4% | 4.01 |
| Avoid clicking suspicious links | 51.4% | 24.9% | 15.1% | 8.6% | 4.19 |
| Regular account statement monitoring | 28.6% | 31.1% | 24.9% | 15.4% | 3.73 |
| Avoid public Wi-Fi for banking | 34.9% | 26.0% | 22.6% | 16.5% | 3.79 |
| Update banking apps regularly | 29.7% | 28.3% | 26.3% | 15.7% | 3.72 |
| Verify caller identity before sharing OTP | 58.3% | 21.7% | 12.6% | 7.4% | 4.31 |
| Report suspicious transactions promptly | 24.3% | 26.6% | 28.0% | 21.1% | 3.54 |
| Use of VPN on public networks | 12.6% | 18.3% | 27.4% | 41.7% | 3.01 |
| Overall Mitigation Behaviour Score | | | | | 3.80 |

***Table 4.4: Frequency of Risk Mitigation Behaviours (N = 350)***

The respondents' overall mean risk mitigation behavior score of 3.80 indicates a fairly active protective posture. OTP sharing vigilance is the most frequently practiced behavior (mean = 4.31), which reflects the significant institutional communication about this particular hazard. Utilizing two-factor authentication (4.01) and avoiding dubious links (4.19) both receive comparatively good scores. The poorest mitigation behaviors, on the other hand, are VPN use on public networks (3.01) and timely reporting of suspicious transactions (3.54), suggesting significant gaps in the adoption of technically complex and procedurally demanding protective measures.

ISSN: 2321-4708
RESEARCH REVIEW
The Academic Research Issue
Open Access, Peer-Reviewed & Refereed Journal
An International Multidisciplinary Journal
Vol.1, Issue: 163, Mar 2026
Paper ID: RRJ012926
www.researchreviewonline.com
Publishing URL: https://www.researchreviewonline.com/issues/volume-1-issue-163-march-2026/RRJ012926

**Regression Analysis: Predictors of Risk Mitigation Behaviour**

Using cybersecurity knowledge and threat perception as the main independent variables and demographic traits as controls, multiple regression analysis was used to investigate the predictors of risk mitigation behavior. The regression results are shown in Table 4.5.

| Predictor Variable | Beta (β) | Std. Error | t-value | p-value | Significance |
|---|---|---|---|---|---|
| Cybersecurity Awareness | 0.412 | 0.063 | 6.54 | < 0.001 | *** |
| Threat Perception (Severity) | 0.287 | 0.071 | 4.04 | < 0.001 | *** |
| Threat Perception (Likelihood) | 0.193 | 0.068 | 2.84 | 0.005 | ** |
| Age (reverse coded) | -0.168 | 0.058 | -2.90 | 0.004 | ** |
| Education Level | 0.214 | 0.072 | 2.97 | 0.003 | ** |
| Digital Banking Experience | 0.176 | 0.064 | 2.75 | 0.006 | ** |
| Gender (Male = 1) | 0.091 | 0.061 | 1.49 | 0.137 | ns |
| Location (Urban = 1) | 0.142 | 0.065 | 2.18 | 0.030 | * |

***Table 4.5: Multiple Regression Analysis Predictors of Risk Mitigation Behaviour $R^2 = 0.61$; Adjusted $R^2 = 0.60$; $F(8, 341) = 66.4$, $p < 0.001$ *** $p < 0.001$; ** $p < 0.01$; * $p < 0.05$; ns = not significant***

The regression model explains 61% of the variance in risk mitigation behavior (R2 = 0.61) and is statistically significant (F = 66.4, p < 0.001). The most potent predictor of self-protective behavior in digital banking scenarios is cybersecurity awareness (β = 0.412, p < 0.001). According to PMT predictions, perceived severity (β = 0.287, p < 0.001) and perceived likelihood (β = 0.193, p < 0.01) are both significant positive predictors. Even after adjusting for awareness and threat perception, age has a significant negative effect (β = -0.168, p < 0.01), suggesting that protective action in older age groups is hampered by factors other than knowledge and motivation. Significant positive factors include education level (β = 0.214, p < 0.01), digital banking experience (β = 0.176, p < 0.01), and urban location (β = 0.142, p < 0.05). After adjusting for other factors, gender does not show up as a significant predictor.

**Findings**

The empirical analysis yields the following principal findings:

→ Overall, Indian digital banking consumers have a moderate level of cybersecurity awareness (mean = 3.18/5), with notable gaps in knowledge of new threat types, especially SIM swap fraud (2.71) and UPI-based social engineering (2.58), which are the two categories of cybercrime that are currently expanding the fastest in India's digital payments market.

→ Perceived threat severity (4.29) consistently surpasses perceived personal vulnerability (3.55) across all threat types, indicating a fairly strong threat perception (mean composite = 3.92/5). The adoption of comprehensive protective behavior is hampered by this bias, which is a structural cognitive barrier.

↳ Risk mitigation behavior is moderate (mean = 3.80/5), with strong adoption of socially reinforced behaviors like link avoidance and OTP vigilance, but notable under-acceptance of technically difficult measures like timely transaction reporting (3.54) and VPN usage (3.01).

↳ The largest predictor of risk mitigation behavior is cybersecurity awareness (β = 0.412, p < 0.001), followed by perceived severity (β = 0.287) and perceived likelihood (β = 0.193). This indicates that Protection Motivation Theory is applicable to the Indian digital banking context.

↳ Age is a significant negative predictor of mitigation behavior (β = -0.168, p < 0.01), with older respondents (51+ years) showing significantly lower awareness scores and mitigation behavior frequencies than younger cohorts. This suggests that targeted cybersecurity education interventions should target this demographic.

ISSN: 2321-4708
RESEARCH REVIEW
The Academic Research Issue
Open Access, Peer-Reviewed & Refereed Journal
An International Multidisciplinary Journal
Vol.1, Issue: 163, Mar 2026
Paper ID: RRJ012926
www.researchreviewonline.com
Publishing URL: https://www.researchreviewonline.com/issues/volume-1-issue-163-march-2026/RRJ012926

- Both awareness and protective behavior are strongly positively predicted by education level and experience with digital banking, indicating that ongoing digital involvement gradually increases cybersecurity competency.
- Due to differences in access to institutional literacy programs, technically advanced device environments, and cybersecurity awareness information, urban respondents display much higher mitigation behavior than semi-urban respondents.

**Conclusion**

The present study provides a comprehensive empirical examination of cybersecurity risks in digital banking in India, with particular emphasis on customer awareness, threat perception, and risk mitigation strategies. In an era marked by rapid digital transformation, the findings underscore that while digital banking has significantly enhanced financial accessibility and convenience, it has also introduced critical vulnerabilities that demand immediate and sustained attention. The study reveals that customer awareness plays a foundational role in shaping cybersecurity behavior. Although a considerable proportion of respondents demonstrate basic knowledge of digital banking operations, gaps persist in their understanding of advanced cyber threats such as phishing, malware, and identity theft. These gaps are more pronounced among older users, less-educated individuals, and those residing in semi-urban areas. This indicates that digital inclusion without corresponding cybersecurity literacy may expose users to heightened risks, thereby undermining the benefits of digital financial services.

The analysis highlights that threat perception significantly influences user behavior. Respondents who exhibit a higher perception of cybersecurity risks are more likely to adopt protective measures such as strong passwords, two-factor authentication, and cautious online practices. However, the study also identifies a mismatch between perceived and actual risks among certain user groups, suggesting that awareness alone is insufficient unless it translates into realistic threat assessment. This finding reinforces the importance of not only educating users about cyber risks but also enabling them to accurately evaluate and respond to such threats. The adoption of risk mitigation strategies among users, although present, remains inconsistent. While widely promoted measures such as OTP-based authentication are commonly used, more proactive practices such as regular monitoring of accounts, updating security settings, and avoiding unsecured networks are not uniformly followed. This inconsistency reflects both behavioral inertia and usability challenges associated with digital security mechanisms. It also emphasizes the need for designing user-friendly and accessible security systems that encourage consistent compliance.

The study also highlights the critical role of financial institutions and regulatory bodies in strengthening cybersecurity frameworks. Banks and fintech companies must go beyond technical safeguards and actively engage in customer education through targeted awareness campaigns, especially for vulnerable segments. Regulatory authorities should continue to refine policies related to data protection, fraud prevention, and customer liability, ensuring that they remain adaptive to evolving cyber threats. Cybersecurity in digital banking is not merely a technological issue but a multidimensional challenge involving human behavior, institutional responsibility, and regulatory oversight. The interplay between awareness, threat perception, and risk mitigation is central to building a secure digital financial ecosystem. Therefore, a collaborative approach involving users, financial institutions, and policymakers is essential to enhance resilience against cyber threats. The study contributes valuable insights for developing effective strategies to promote safe digital banking practices and supports the broader goal of sustainable and secure digital financial inclusion in India.

ISSN: 2321-4708
RESEARCH REVIEW
The Academic Research Issue
Open Access, Peer-Reviewed & Refereed Journal
An International Multidisciplinary Journal
Vol.1, Issue: 163, Mar 2026
Paper ID: RRJ012926
www.researchreviewonline.com
Publishing URL: https://www.researchreviewonline.com/issues/volume-1-issue-163-march-2026/RRJ012926

## REFERENCES

Bose, I., & Leung, A. C. M. (2014). Do phishing alerts impact global corporations? A firm value analysis. Decision Support Systems, 64, 67–78.

Bouveret, A. (2018). Cyber risk for the financial sector: A framework for quantitative assessment (IMF Working Paper WP/18/143). International Monetary Fund.

CERT-In. (2024). Annual report 2023: Indian Computer Emergency Response Team. Ministry of Electronics and Information Technology, Government of India.

Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2009). Information security: The moving target. Computers & Security, 28(3–4), 189–198.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. Journal of the Association for Information Systems, 11(7), 394–413.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. Journal of Experimental Social Psychology, 19(5), 469–479.

Malhotra, P., & Singh, B. (2019). Determinants of mobile banking adoption in India: An empirical analysis. International Journal of Bank Marketing, 38(3), 522–545.

National Centre for Financial Education (NCFE). (2023). National financial literacy and inclusion survey 2022–23. NCFE India.

National Payments Corporation of India (NPCI). (2024). UPI product statistics: Annual report 2023–24. NPCI.

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559–569.

Poonia, A. S., Chauhan, R., & Bhatt, A. (2021). Cyber security awareness among mobile banking users in India: An empirical analysis. Journal of Information Security and Applications, 58, 102774.

Reserve Bank of India (RBI). (2022). Report on trend and progress of banking in India 2021–22. RBI Publications.

Reserve Bank of India (RBI). (2023). Annual report 2022–23. Reserve Bank of India.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1), 93–114.

Shey, H. (2012). Understanding the state of data security and privacy: A review of enterprise security practices. Forrester Research.

Singh, S., & Pandey, S. K. (2020). Cyber threats and cyber frauds in banking sector of India: A review. International Journal of Advanced Science and Technology, 29(5), 4781–4791.

ISSN: 2321-4708
RESEARCH REVIEW
The Academic Research Issue
Open Access, Peer-Reviewed & Refereed Journal
An International Multidisciplinary Journal
Vol.1, Issue: 163, Mar 2026
Paper ID: RRJ012926
www.researchreviewonline.com
Publishing URL: https://www.researchreviewonline.com/issues/volume-1-issue-163-march-2026/RRJ012926

Sood, A. K., & Enbody, R. J. (2013). Targeted cyberattacks: A superset of advanced persistent threats. IEEE Security & Privacy, 11(1), 54–61.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decision Support Systems, 51(3), 576–586.

Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. Information Systems Security, 16(6), 315–331.

Yoon, C. (2018). Extending the TAM for a World Wide Web context. Information & Management, 55(4), 448–458.