



International Journal of Research Publication and Reviews

Journal Homepage: www.ijrpr.com ISSN 2582-7421

Examining the Role of Generative AI in Preventing Deepfake Financial Fraud: Challenges and Opportunities in the FinTech Ecosystem

Ms. Aparna Saxena¹, Dr. D. Praveenadevi²

¹ Research Scholar, BBA Department, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India.

Email- aparnasaxena3006@gmail.com

² Assistant Professor, Business School, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India.

Email - praveenadevid86@kluniversity.in

ABSTRACT

Generative Artificial Intelligence has made deepfake financial fraud more sophisticated, yet it also gives institutions new ways to detect and prevent it. This study examines the role of Generative AI capabilities in preventing deepfake financial fraud in the FinTech ecosystem, with AI-based fraud detection and prevention as the mediating variable and Data Privacy and Security as the moderating variable in the conceptual framework. The study follows a quantitative, cross-sectional design. A structured questionnaire with five-point Likert items produced 130 responses (N = 130), which were analysed in Microsoft Excel using Cronbach's alpha, chi-square tests, one-way ANOVA, linear regression and moderated regression. All four constructs were reliable (Cronbach's $\alpha = .850-.902$), and respondents' perceptions were generally favourable, with construct means between 3.67 and 3.99 on a five-point scale. Generative AI capabilities had a significant positive relationship with AI-based fraud detection and prevention ($\beta = .838$, $R^2 = .702$, $p < .001$). AI-based fraud detection and prevention was significantly and positively related to deepfake financial fraud prevention ($\beta = .858$, $R^2 = .737$, $p < .001$), and Generative AI capabilities were also directly related to deepfake financial fraud prevention ($\beta = .852$, $R^2 = .726$, $p < .001$). Hypotheses H1 to H3 were therefore supported. Data Privacy and Security did not significantly moderate these relationships (interaction $p = .588-.857$), so H4 was not supported, although it was positively associated with perceived deepfake financial fraud prevention. Perceptions differed most by age group ($\chi^2(2) = 13.64$, $p = .001$). Since the study measures perceptions and the sample is dominated by young respondents, the results show associations, not causal effects or actual fraud outcomes.

Keywords: Generative AI; Deepfake; Financial Fraud Prevention; AI-Based Fraud Detection; FinTech; Data Privacy and Security

1. Introduction

Digital financial services have become central to how individuals and businesses pay, save, borrow and transact. Banks and FinTech platforms increasingly rely on remote identity checks, video-based onboarding, voice-based authentication and real-time payments, which allow customers to use financial services without visiting a branch. The same convenience, however, widens the range of channels through which fraud can be attempted. A fraudster no longer needs physical access to a customer or an institution, only convincing evidence of identity, such as a face, a voice or a document, delivered through a digital channel. As more financial activity moves online, protecting these channels has become a major concern for institutions, regulators and customers alike.

Generative Artificial Intelligence has made this concern sharper, because it can produce convincing synthetic faces, voices, documents and messages. Kurshan et al. (2024) describe how the growing use of Generative AI in financial crime challenges existing detection systems, and they emphasise the need for adaptive, co-evolutionary AI and closer industry cooperation. Marwick et al. (2026) show that policy responses to Generative AI-enabled deepfake financial fraud remain fragmented across jurisdictions. Studies have also documented specific attack settings, including deepfake-driven fraud in onboarding and KYC (Delva Benavides et al., 2026) and voice-cloning attacks on voice-based authentication (Jayakannan, 2025). The consequences go beyond direct losses: Adegoke and Adegoke (2026) examine how AI-enabled fraud affects consumer trust and digital financial adoption in Nigeria.

Generative AI is therefore both a source of risk and a resource for defence. Generative models have been applied to banking fraud detection (Kumar, 2025), to real-time transaction screening (Dixit, 2024), and to data augmentation for imbalanced fraud data, where Shan et al. (2026) report improved detection across several classifiers. Igba et al. (2025) examine synthetic data for identity-fraud detection, and large language models have been combined with reinforcement learning and on-device processing for fraud detection (Hacini et al., 2025; Senevirathna & Sumanathilaka, 2025). Work on deepfake-specific detection includes multimodal and explainable frameworks (Amaresam, 2024; Rath, 2026; Rahat et al., 2026), federated and privacy-preserving approaches for Video-KYC (Rawat et al., 2026) and hybrid models for deepfake voice detection in banking calls (Gokul et al., 2026). Taken together, these studies suggest that AI-based fraud detection and prevention is where the capabilities of Generative AI are put to work against deepfake financial fraud.

The same literature also points to unresolved challenges. Data privacy, explainability and adversarial attacks are identified as concerns even where detection improves (Amaresam, 2024; Kumar, 2025), and Rawat et al. (2026) design their Video-KYC framework around data privacy and regulatory compliance. Zeng et al. (2026) stress lifecycle-aware security and robust AI systems in financial applications. Across the literature, then, data privacy and security appear less as a detection technique and more as a condition that decides whether AI-based fraud prevention can be trusted and deployed.

Despite this growing body of work, most of the studies are technical, conceptual or policy-oriented. Many of the technical studies are validated on benchmark, public or synthetic datasets, and the conceptual and review studies report no primary empirical testing of their proposals. The only study in the reviewed set that surveyed users directly is Adegoke and Adegoke (2026), whose focus was fraud exposure, trust and adoption and not the perceived role of Generative AI in preventing deepfake fraud. Few studies examine how stakeholders perceive the links between Generative AI capabilities, AI-based fraud detection and prevention, and deepfake financial fraud prevention, or whether concern for data privacy and security changes those links. Trust and adoption influence whether protective technologies are actually used, so perceptions are a relevant form of evidence, and an integrated empirical test of these relationships is needed.

This study addresses that need. It examines the role of Generative AI capabilities in preventing deepfake financial fraud in the FinTech ecosystem, with AI-based fraud detection and prevention as a mediating variable and Data Privacy and Security as a moderating, or contextual, variable. Using primary questionnaire-based empirical evidence from 130 responses, it tests four hypotheses through chi-square tests, one-way ANOVA, linear regression and moderated regression. The questionnaire records respondents' perceptions and assessments, and it does not measure actual fraud incidents, losses or detection accuracy. Its contribution is to bring the three fraud-prevention constructs and the privacy and security context into a single framework and test them with primary data. The rest of the paper sets out the research gap, problem statement, research questions, conceptual framework, objectives and hypotheses, then reviews the literature, describes the methodology, reports the results, and then discusses the implications, limitations and conclusions.

2. Research Gap

Although existing studies have extensively examined AI-based financial fraud detection and deepfake detection using machine learning, deep learning, multimodal analysis, synthetic data, and Generative AI techniques, the existing literature remains fragmented across individual fraud types, detection technologies, and governance dimensions. Most studies focus primarily on technical detection performance, while relatively limited research integrates Generative AI capabilities with AI-based fraud detection and prevention and examines their contribution to preventing deepfake financial fraud within the broader FinTech ecosystem. Furthermore, challenges related to data privacy and security, explainability, regulatory compliance, scalability, and the rapidly evolving nature of Generative AI-enabled fraud are often addressed independently rather than within an integrated empirical framework. Therefore, there is a need for empirical research that examines the relationships among Generative AI capabilities, AI-based fraud detection and prevention, and deepfake financial fraud prevention, while considering Data Privacy and Security as a contextual factor influencing these relationships.

3. Problem Statement

Generative AI has enabled sophisticated forms of deepfake financial fraud, creating new challenges for financial institutions and FinTech platforms. Although existing studies have examined AI-based fraud detection, deepfake detection, and related security technologies, limited research integrates Generative AI capabilities, AI-based fraud detection and prevention, and deepfake financial fraud prevention within a single framework. Therefore, this study examines the role of Generative AI in preventing deepfake financial fraud while considering Data Privacy and Security as an important contextual factor in the FinTech ecosystem.

4. Research Questions

1. How do Generative AI capabilities influence AI-based fraud detection and prevention in the FinTech ecosystem?
2. To what extent do AI-based fraud detection and prevention capabilities contribute to the prevention of deepfake financial fraud?
3. How does Data Privacy and Security influence the relationships between Generative AI capabilities, AI-based fraud detection and prevention, and deepfake financial fraud prevention?

5. Conceptual Framework

The conceptual framework, shown in Figure 1, contains four variables. Generative AI Capabilities, which include deepfake detection, anomaly detection, multimodal analysis, intelligent automation, synthetic data generation, and adaptive and real-time learning, is the independent variable. AI-Based Fraud Detection and Prevention Capabilities, covering identity verification and authentication, deepfake content analysis, risk scoring and alerts, real-time monitoring, and decision support and response, is the mediating variable. Deepfake Financial Fraud Prevention, conceptually reflected in reduced fraud incidents, improved detection accuracy, fewer false positives, faster response and enhanced customer trust, is the dependent variable. Data Privacy and Security, which covers data privacy, scalability and cost, model accuracy and bias, explainability and transparency, regulatory compliance, and talent and skill gaps, is the moderating or contextual variable. Generative AI Capabilities are linked to AI-Based Fraud Detection and Prevention, which is linked

to Deepfake Financial Fraud Prevention. Generative AI Capabilities are also linked directly to Deepfake Financial Fraud Prevention, and Data Privacy and Security acts on these relationships.

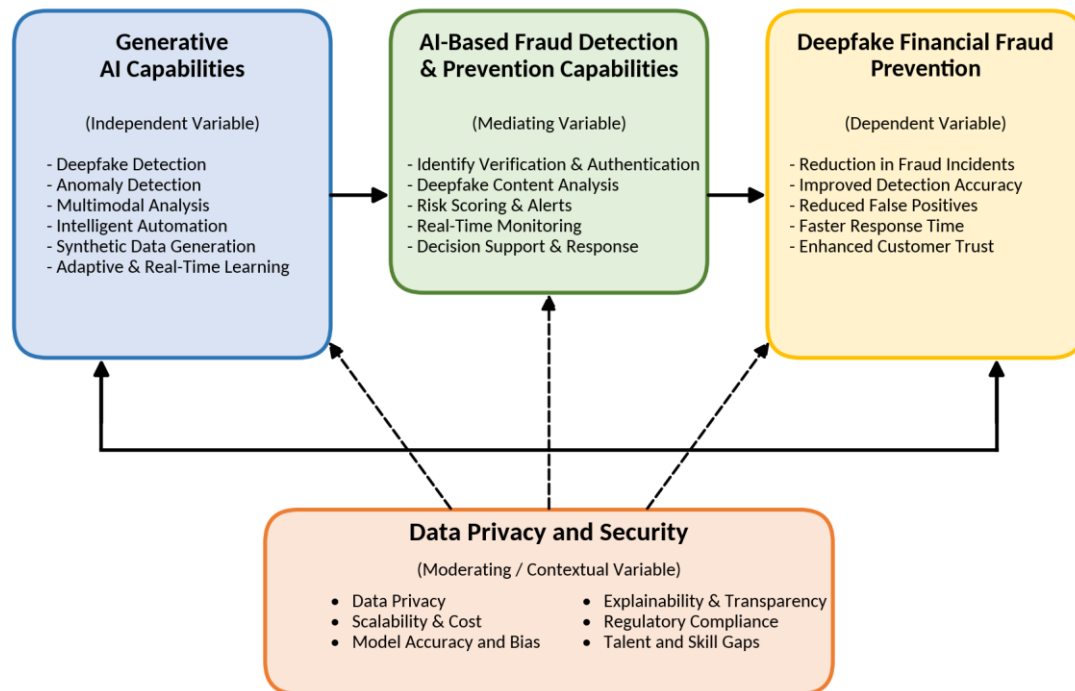


Figure 1. Conceptual framework of the study

6. Research Objectives

1. To conceptualise the relationships among Generative AI capabilities, AI-based fraud detection and prevention, and deepfake financial fraud prevention in the FinTech ecosystem.
2. To assess the influence of Generative AI capabilities on AI-based fraud detection and prevention capabilities.
3. To evaluate the contribution of AI-based fraud detection and prevention capabilities to deepfake financial fraud prevention.
4. To determine the direct influence of Generative AI capabilities on deepfake financial fraud prevention.
5. To examine the moderating role of Data Privacy and Security in the relationships among Generative AI capabilities, AI-based fraud detection and prevention, and deepfake financial fraud prevention.

7. Hypotheses

H1: Generative AI Capabilities and AI-Based Fraud Detection and Prevention

H₀₁: Generative Artificial Intelligence capabilities have no significant relationship with AI-based fraud detection and prevention capabilities.

H₁₁: Generative Artificial Intelligence capabilities have a significant positive relationship with AI-based fraud detection and prevention capabilities.

H2: AI-Based Fraud Detection and Prevention and Deepfake Financial Fraud Prevention

H₀₂: AI-based fraud detection and prevention capabilities have no significant relationship with deepfake financial fraud prevention.

H₁₂: AI-based fraud detection and prevention capabilities have a significant positive relationship with deepfake financial fraud prevention.

H3: Direct Relationship between Generative AI Capabilities and Deepfake Financial Fraud Prevention

H₀₃: Generative Artificial Intelligence capabilities have no significant direct relationship with deepfake financial fraud prevention.

H₁₃: Generative Artificial Intelligence capabilities have a significant positive direct relationship with deepfake financial fraud prevention.

H4: Moderating Role of Data Privacy and Security

H₀₄: Data Privacy and Security does not significantly moderate the relationships among Generative Artificial Intelligence capabilities, AI-based fraud detection and prevention, and deepfake financial fraud prevention.

H₁₄: Data Privacy and Security significantly moderates the relationships among Generative Artificial Intelligence capabilities, AI-based fraud detection and prevention, and deepfake financial fraud prevention.

8. Review of Literature

The following studies form the secondary research base of this paper. The studies are reviewed in the order presented below.

Shan (2025) examined AI-powered fraud detection in banking and found that AI/ML-based techniques can outperform traditional rule-based systems in detecting deepfake, identity, voice, and document-related fraud.

Rath (2026) developed an adversarial-resilient and explainable AI framework using deep learning, multimodal fusion, adversarial training, and XAI to improve deepfake-aware fraud detection in financial systems.

Rahat et al. (2026) proposed a multimodal machine-learning framework for identifying deepfake-driven identity abuse, authentication evasion, and customer impersonation across the U.S. banking customer journey.

Amamesam (2024) presented a layered, multimodal AI framework for deepfake detection and digital fraud prevention across banking and fintech. The study reported high detection performance and stressed the importance of human review, privacy, explainability, and real-time deployment.

Marwick et al. (2026) examined policy responses to Generative AI-enabled deepfake financial fraud across multiple jurisdictions. The authors argued for stronger cross-sector accountability and coordinated regulatory measures.

Kurshan et al. (2024) looked at the growing use of Generative AI in financial crime and the challenges it poses for existing detection systems. The study emphasised adaptive, co-evolutionary AI and greater industry cooperation to address emerging AI-driven financial threats.

Delva Benavides et al. (2026) proposed a risk-based framework for addressing deepfake fraud in FinTech onboarding and KYC. The framework stresses authentication, traceability, privacy and liability.

Zeng et al. (2026) surveyed trustworthy AI risks in FinTech across the AI lifecycle, including deepfake-based KYC attacks. The survey called for lifecycle-aware security and robust AI systems in financial applications.

Adegoke and Adegoke (2026) examined the effects of AI-enabled fraud on consumer trust and digital financial adoption in Nigeria. The study pointed to the prevalence of deepfakes, voice cloning, phishing and synthetic identity fraud, and stressed AI-based detection and awareness as key mitigation measures.

Kumar (2025) explored the use of Generative AI for banking fraud detection using VAE, GAN, and LLM-based approaches. The study reported improved fraud detection but also identified challenges related to privacy, explainability, and adversarial attacks.

Dixit (2024) proposed a real-time GAN-based framework for FinTech fraud detection using CNN/RNN architectures and adversarial training. The study reported improved detection of novel fraud patterns, fewer false positives and real-time transaction screening.

Shan et al. (2026) proposed GAN-FFAD to address data imbalance and scarcity in financial fraud detection. The study found that GAN-based data augmentation improved fraud detection performance across multiple machine-learning classifiers.

Senevirathna and Sumanathilaka (2025) developed a lightweight LLM-based framework for privacy-preserving financial fraud detection on mobile devices. The study demonstrated high detection accuracy with low latency, highlighting the potential of on-device AI for real-time fraud detection.

Hacini et al. (2025) proposed an LLM-assisted reinforcement learning framework for financial fraud detection. The study found that combining LLM embeddings with reinforcement learning can improve fraud detection, particularly for heterogeneous transaction data.

Rawat et al. (2026) proposed a privacy-preserving federated framework for deepfake fraud detection in financial Video-KYC systems. The study showed high detection performance while addressing data privacy, real-time detection, and regulatory compliance.

Jayakannan (2025) investigated vulnerabilities in voice-based financial authentication caused by AI voice cloning. The study proposed combining behavioural biometrics, context-aware authentication, and real-time synthetic voice detection to prevent voice-based fraud.

Gokul et al. (2026) developed a real-time AI/ML system for detecting deepfake voices in banking calls. The study used a hybrid CNN-RNN model to identify AI-generated speech and trigger alerts for potential voice-cloning scams.

Igba et al. (2025) looked at Generative AI, synthetic data generation, identity fraud detection, anomaly detection, and biometric verification. The study pointed to the potential of synthetic data to improve fraud detection and financial cybersecurity.

Research gaps identified in the reviewed studies

The studies reviewed above share a common set of gaps. First, several are conceptual, review-based or policy-based and report no primary empirical testing of their proposals, for example Shan (2025), Marwick et al. (2026), Kurshan et al. (2024), Delva Benavides et al. (2026), Zeng et al. (2026), Kumar (2025), Dixit (2024) and Igba et al. (2025). Second, the technical studies are mostly validated on benchmark, public or synthetic datasets rather than live institutional data, for example Rath (2026), Shan et al. (2026), Senevirathna and Sumanathilaka (2025), Hacini et al. (2025), Rawat et al. (2026) and Gokul et al. (2026). Third, privacy, explainability, regulatory compliance and real-time scalability are repeatedly named as unresolved issues (Amaresam, 2024; Dixit, 2024; Kumar, 2025; Zeng et al., 2026). Finally, the only study in the set that surveyed users directly is Adegoke and Adegoke (2026), who studied 210 digital finance users in Nigeria, but their focus was fraud exposure, trust and adoption rather than the perceived role of Generative AI in preventing deepfake fraud. These gaps support the choice of a primary, questionnaire-based test of the integrated framework in this study.

9. Research Methodology

9.1 Research design

The study uses a quantitative, cross-sectional research design supported by secondary literature. A structured, self-administered questionnaire was the primary data collection instrument. Because the questionnaire records respondents' agreement with statements on a five-point scale, the results describe respondents' perceptions and assessments of the study variables. They do not measure actual fraud incidents, financial losses, detection accuracy, false-positive rates or response times.

9.2 Population, Sample and Data Collection

The study considered a population of 182 respondents for determining the required sample size. The sample size was calculated using Yamane's formula at a 5% level of allowable error:

$$n = N / [1 + N(e)^2]$$

where $N = 182$ and $e = 0.05$. The calculated minimum sample size was approximately 125 respondents. The structured questionnaire yielded 130 responses, and all of them were included in the final analysis. Primary data were collected through non-probability convenience sampling. The demographic characteristics of the respondents are presented in Section 10.1.

9.3 Instrument and measurement

The questionnaire has two parts. Part A collects five demographic items: age (Q1), gender (Q2), educational qualification (Q3), occupation (Q4) and frequency of use of digital financial services (Q5). Part B contains 25 statements (Q6–Q30) rated on a five-point Likert scale, where 1 is Strongly Disagree and 5 is Strongly Agree. Items Q11–Q30 form four constructs of five items each, which correspond to the variables in the conceptual framework, as shown in Table 1. Items Q6–Q10 are integrated relationship and perception statements. They are reported descriptively in Section 10.2 and are not included in any construct score. Each construct score is the mean of its five items. The internal consistency of each construct was assessed with Cronbach's alpha (Section 10.3). Discriminant validity was not tested (Section 13).

Table 1. Constructs, questionnaire items and framework role

Construct	Items	Role in framework	Example item
Generative AI Capabilities	Q11–Q15	Independent variable	Generative AI can help identify unusual or suspicious financial activities.
AI-Based Fraud Detection and Prevention	Q16–Q20	Mediating variable	AI-based systems can help verify customer identities and prevent fraudulent activities.
Deepfake Financial Fraud Prevention	Q21–Q25	Dependent variable	Generative AI can help identify manipulated videos and images used in financial fraud.
Data Privacy and Security	Q26–Q30	Moderating variable	Strong data security can increase trust in AI-based fraud detection and prevention systems.

9.4 Data analysis

All calculations were carried out in Microsoft Excel using functions such as COUNTIFS, CHIDIST, FDIST, TDIST, CORREL and LINEST, and the accompanying workbook retains every formula. The techniques were as follows.

- **Descriptive statistics and reliability:** frequencies, percentages, means, standard deviations, skewness, kurtosis, Pearson correlations and Cronbach's alpha for each construct. An alpha of .70 or above was taken as acceptable.
- **Chi-square tests of independence:** each demographic variable was cross-tabulated with the level of perceived deepfake financial fraud prevention, with High defined as a construct mean of 4.00 or above and Low/Moderate as below 4.00. The same cut-off was used to cross-tabulate the levels of the constructs that correspond to H1, H2 and H3. Pearson χ^2 without continuity correction and Cramér's V are reported, and expected cell counts were checked against the minimum of 5. To avoid very small cells, age was grouped as up to 25, 26–35 and above 35; occupation as student and working/other; and usage frequency as daily, several times a week and monthly or less.
- **One-way ANOVA:** differences in the four construct scores across the same grouping variables, with η^2 as the effect size and Bonferroni-adjusted pairwise comparisons for factors with more than two groups. Because 20 ANOVAs were run, the Bonferroni-adjusted threshold of .0025 is also shown.
- **Linear regression for H1, H2 and H3:** three simple linear regressions of the relevant outcome on its predictor, reporting B, standard error, standardised β , t, p, R^2 and F. A hypothesis was supported when the coefficient was positive and $p < .05$.
- **Moderated regression for H4:** for each of the three relationships in the framework, the predictor and Data Privacy and Security were mean-centred and entered in Step 1, and their product term was added in Step 2. H04 is rejected only if at least one interaction term is significant at $p < .05$ with a significant change in R^2 .

The significance level was $\alpha = .05$ throughout. Because Excel does not provide some diagnostics, a few supplementary checks were run outside Excel and are identified where they are reported. These were the Levene, Shapiro–Wilk and Breusch–Pagan tests, Kruskal–Wallis tests, a permutation check and a bootstrap confidence interval.

10. Data Analysis and Results

10.1 Respondent profile

Table 2. Demographic profile of respondents (N = 130)

Characteristic	Category	n	%
Age	Below 18	8	6.2%
	18–25	96	73.8%
	26–35	12	9.2%
	36–45	9	6.9%
	Above 45	5	3.8%
Gender	Female	99	76.2%
	Male	31	23.8%
Educational qualification	Higher Secondary	16	12.3%
	Undergraduate	96	73.8%
	Postgraduate	18	13.8%
Occupation	Student	93	71.5%
	Employed	18	13.8%
	Professional	12	9.2%
	Self-employed/Business	4	3.1%
	Other	3	2.3%
Usage of digital financial services	Daily	60	46.2%
	Several times a week	39	30.0%
	Several times a month	18	13.8%
	Rarely	13	10.0%

Note. Percentages may not sum to 100 because of rounding.

Most respondents are young: 73.8% are aged 18–25 and a further 6.2% are below 18. Women make up 76.2% of the sample, and 73.8% hold or are pursuing an undergraduate qualification. Students account for 71.5% of respondents, and the remaining 28.5% are employed, professionals, self-employed or in other occupations. Regular use of digital financial services is common, with 46.2% using them daily and 30.0% several times a week. The sample is therefore predominantly young and student-based, which should be kept in mind when interpreting the findings, as discussed in Section 13.

10.2 Descriptive statistics

Table 3. Descriptive statistics of the constructs on a 1–5 scale

Construct	Mean	SD	Skewness	Kurtosis	Min–Max	% Agree / Strongly agree
Generative AI Capabilities (Q11–Q15)	3.81	0.82	–1.24	2.46	1.0–5.0	70.3%
AI-Based Fraud Detection and Prevention (Q16–Q20)	3.67	0.88	–0.75	1.00	1.0–5.0	61.4%
Deepfake Financial Fraud Prevention (Q21–Q25)	3.68	0.86	–0.85	1.11	1.0–5.0	62.5%
Data Privacy and Security (Q26–Q30)	3.99	0.96	–1.07	0.71	1.0–5.0	71.2%

Note. N = 130. “% Agree / Strongly agree” is the share of all item responses, 5 items × 130 respondents, coded 4 or 5.

All four construct means are above the neutral midpoint of 3.00, ranging from 3.67 for AI-Based Fraud Detection and Prevention to 3.99 for Data Privacy and Security. Respondents were most favourable towards Data Privacy and Security, where 71.2% of item responses were Agree or Strongly agree, followed by Generative AI Capabilities at 70.3%. The distributions are negatively skewed, with skewness between –1.24 and –0.75. This is common for agreement scales and shows that many respondents chose the upper categories. Table 4 gives the mean and standard deviation of every statement from Q6 to Q30. The five integrated perception items, Q6 to Q10, are not part of any construct. Their means range from 3.52 to 3.65, and between 51.5% and 62.3% of respondents agreed or strongly agreed with them, which is in the same favourable direction as the construct scores.

Table 4. Item-level descriptive statistics for Q6–Q30 (N = 130)

Item	Statement	Mean	SD	% Agree / Strongly agree
Integrated relationship and perception items, not included in any construct score				
Q6	Generative AI capabilities can support AI-based financial fraud detection and prevention.	3.52	0.99	51.5%
Q7	AI-based fraud detection and prevention can contribute to preventing deepfake financial fraud.	3.60	1.05	62.3%
Q8	Generative AI can contribute directly to the prevention of deepfake financial fraud.	3.53	0.97	53.8%
Q9	Generative AI, AI-based fraud detection, and deepfake financial fraud prevention are interconnected in the FinTech ecosystem.	3.62	1.01	56.9%
Q10	Integrating Generative AI with AI-based fraud detection can strengthen deepfake financial fraud prevention.	3.65	1.15	59.2%
Generative AI Capabilities				
Q11	Generative AI can help identify unusual or suspicious financial activities.	3.73	1.10	67.7%
Q12	Generative AI can analyze different types of financial information to support fraud detection.	3.71	1.08	67.7%
Q13	Generative AI can identify new and emerging patterns of financial fraud.	3.98	0.96	80.8%
Q14	Generative AI can improve the speed of financial fraud detection.	3.80	1.04	68.5%
Q15	Generative AI can improve the overall capabilities of AI-based fraud detection and prevention systems.	3.84	1.03	66.9%

Item	Statement	Mean	SD	% Agree / Strongly agree
AI-Based Fraud Detection and Prevention				
Q16	AI-based systems can help verify customer identities and prevent fraudulent activities.	3.66	1.12	62.3%
Q17	AI-based systems can detect suspicious transactions associated with financial fraud.	3.71	1.06	63.1%
Q18	AI-based systems can detect deepfake-related financial fraud.	3.47	1.03	47.7%
Q19	Real-time AI-based monitoring can help prevent deepfake financial fraud.	3.76	1.15	64.6%
Q20	AI-based fraud detection and prevention can reduce the risk of deepfake financial fraud.	3.76	1.13	69.2%
Deepfake Financial Fraud Prevention				
Q21	Generative AI can help identify manipulated videos and images used in financial fraud.	3.61	1.10	61.5%
Q22	Generative AI can help identify AI-generated or cloned voices used in financial fraud.	3.75	1.14	62.3%
Q23	Generative AI can help verify whether digital content used in financial transactions is genuine.	3.68	1.07	59.2%
Q24	Generative AI can help financial institutions respond quickly to deepfake financial fraud.	3.81	1.04	67.7%
Q25	Generative AI can directly strengthen the prevention of deepfake financial fraud.	3.55	1.07	61.5%
Data Privacy and Security				
Q26	Protecting personal data is important when using Generative AI for financial fraud prevention.	3.88	1.25	69.2%
Q27	Strong data security can increase trust in AI-based fraud detection and prevention systems.	3.91	1.22	65.4%
Q28	Data privacy concerns can affect the use of Generative AI for financial fraud prevention.	3.99	0.92	74.6%
Q29	Financial institutions should follow data protection regulations when using AI for fraud prevention.	4.17	1.09	75.4%
Q30	Strong data privacy and security measures can support the effective use of Generative AI for preventing deepfake financial fraud.	4.00	1.16	71.5%

Note. Items were rated from 1, Strongly Disagree, to 5, Strongly Agree. % Agree / Strongly agree is the share of the 130 respondents who selected 4 or 5.

10.3 Reliability analysis

Table 5. Reliability analysis using Cronbach's alpha

Construct	Items	Cronbach's α	Range of α if an item is deleted
Generative AI Capabilities	5	.850	.803–.839
AI-Based Fraud Detection and Prevention	5	.860	.809–.847
Deepfake Financial Fraud Prevention	5	.857	.806–.859
Data Privacy and Security	5	.902	.870–.888

Note. N = 130. A value of .70 or above is taken as acceptable.

Cronbach's alpha was .850 for Generative AI Capabilities, .860 for AI-Based Fraud Detection and Prevention, .857 for Deepfake Financial Fraud Prevention and .902 for Data Privacy and Security. All values exceed .70, so the five items of each construct are internally consistent. Deleting any single

item would leave alpha above .80 for every construct. The only item whose deletion would raise alpha at all is Q25 of Deepfake Financial Fraud Prevention, and then only by .002.

Table 6. Pearson correlations among constructs

Construct	1	2	3	4
1. Generative AI Capabilities	—	.838	.852	.824
2. AI-Based Fraud Detection and Prevention		—	.858	.755
3. Deepfake Financial Fraud Prevention			—	.782
4. Data Privacy and Security				—

Note. N = 130. All correlations are significant at $p < .001$.

The constructs are strongly and positively correlated, with r between .755 and .858. This fits the relationships proposed in the framework. The size of the correlations also suggests that respondents who rated one construct favourably tended to rate all of them favourably.

10.4 Chi-square tests

10.4.1 Demographic characteristics and the level of perceived deepfake financial fraud prevention

Table 7. Chi-square tests of demographic characteristics and the level of perceived deepfake financial fraud prevention

Characteristic	Group (n)	% High on DFP	χ^2	df	p	V
Age group	Up to 25 (104)	44.2%	13.64	2	.001	.324
	26–35 (12)	100.0%				
	Above 35 (14)	42.9%				
Gender	Female (99)	44.4%	3.81	1	.051	.171
	Male (31)	64.5%				
Education	Higher Secondary (16)	12.5%	11.14	2	.004	.293
	Undergraduate (96)	52.1%				
	Postgraduate (18)	66.7%				
Occupation	Student (93)	44.1%	3.46	1	.063	.163
	Working / Other (37)	62.2%				
Usage frequency	Daily (60)	46.7%	2.46	2	.293	.138
	Several times a week (39)	43.6%				
	Monthly or less (31)	61.3%				

Note. “% High on DFP” is the share of each group whose Deepfake Financial Fraud Prevention mean is 4.00 or above; the overall share is 49.2%. N = 130 for every test. No cell had an expected count below 5, and the smallest expected count was 5.91, in the age-group table. V is Cramér’s V.

Age group was significantly associated with the level of perceived deepfake financial fraud prevention, $\chi^2(2, N = 130) = 13.64$, $p = .001$, $V = .324$, which is a medium association. All 12 respondents aged 26–35 rated deepfake financial fraud prevention highly, compared with 44.2% of those up to 25 and 42.9% of those above 35. Education was also significantly associated, $\chi^2(2, N = 130) = 11.14$, $p = .004$, $V = .293$. Only 12.5% of higher-secondary respondents rated it highly, compared with 52.1% of undergraduates and 66.7% of postgraduates.

Gender, $\chi^2(1, N = 130) = 3.81$, $p = .051$, $V = .171$, and occupation, $\chi^2(1, N = 130) = 3.46$, $p = .063$, $V = .163$, were not significant at the .05 level, although a higher share of male respondents rated deepfake financial fraud prevention highly than of female respondents (64.5% against 44.4%), and the same was true of working respondents compared with students (62.2% against 44.1%). Frequency of use was not significantly associated either, $\chi^2(2, N = 130) = 2.46$, $p = .293$, $V = .138$.

Because five demographic tests were run, a Bonferroni-adjusted threshold of .01 is a more cautious benchmark, and at that level age group and education remain significant. The age-group and education tables satisfied the expected-count requirement, and a supplementary permutation test run outside Excel gave the same conclusions (age group $p < .001$; education $p = .003$). The groups are very unequal in size. For example, 104 respondents are aged up to

25, compared with 12 aged 26–35 and 14 above 35, and 99 are female compared with 31 male. These results therefore describe associations in this sample and should not be generalised.

10.4.2 Levels of the constructs

Table 8. Chi-square tests between construct levels

High versus Low/Moderate cross-tabulation	Related hypothesis	% High on outcome: High vs Low/Mod.	$\chi^2(1)$	p	V
Generative AI Capabilities level × AI-Based Fraud Detection and Prevention level	H1	63.3% vs 13.7%	30.92	< .001	.488
AI-Based Fraud Detection and Prevention level × Deepfake Financial Fraud Prevention level	H2	87.7% vs 19.2%	60.16	< .001	.680
Generative AI Capabilities level × Deepfake Financial Fraud Prevention level	H3	72.2% vs 13.7%	42.33	< .001	.571
Data Privacy and Security level × Deepfake Financial Fraud Prevention level	Context	66.7% vs 14.0%	31.99	< .001	.496

Note. V is Cramér's V. N = 130. No cell had an expected count below 5, and the smallest was 21.17. The first percentage is for respondents rating the predictor construct High, the second for the rest.

Respondents who rated one construct highly were much more likely to rate the next construct highly. Among respondents with a high rating of Generative AI Capabilities, 63.3% also rated AI-Based Fraud Detection and Prevention highly, compared with 13.7% of the rest ($\chi^2(1) = 30.92$, $p < .001$, $V = .488$). The corresponding figures were 87.7% and 19.2% for AI-Based Fraud Detection and Prevention and Deepfake Financial Fraud Prevention ($\chi^2(1) = 60.16$, $V = .680$), 72.2% and 13.7% for Generative AI Capabilities and Deepfake Financial Fraud Prevention ($\chi^2(1) = 42.33$, $V = .571$), and 66.7% and 14.0% for Data Privacy and Security and Deepfake Financial Fraud Prevention ($\chi^2(1) = 31.99$, $V = .496$). All p-values were below .001. These associations point in the direction of H1, H2 and H3. The hypothesis decisions, however, rest on the regression analysis in Section 10.6, because dividing scores into two levels discards information.

10.5 One-way ANOVA

Table 9. One-way ANOVA of construct scores by demographic factors, F (p)

Grouping factor (df)	Generative AI Capabilities	AI-Based Fraud Detection and Prevention	Deepfake Financial Fraud Prevention	Data Privacy and Security
Age group (2, 127)	7.62 (< .001) ‡	3.59 (.030) †	5.92 (.003) †	5.83 (.004) †
Gender (1, 128)	7.09 (.009) †	4.51 (.036) †	4.02 (.047) †	6.80 (.010) †
Education (2, 127)	2.10 (.127)	0.92 (.403)	3.62 (.030) †	3.71 (.027) †
Occupation (1, 128)	6.97 (.009) †	3.98 (.048) †	3.16 (.078)	7.94 (.006) †
Usage frequency (2, 127)	1.68 (.191)	4.19 (.017) †	3.02 (.052)	1.30 (.277)

Note. † $p < .05$; ‡ $p < .0025$, the Bonferroni-adjusted threshold for 20 tests. N = 130 for every test. Groups were age: up to 25, 26–35 and above 35; gender: female and male; education: higher secondary, undergraduate and postgraduate; occupation: student and working/other; usage: daily, several times a week and monthly or less.

Table 10. Mean and standard deviation of construct scores by group

Factor	Group	n	Generative AI Capabilities	AI-Based Fraud Detection and Prevention	Deepfake Financial Fraud Prevention	Data Privacy and Security
Age group	Up to 25	104	3.75 (0.73)	3.60 (0.81)	3.61 (0.80)	3.87 (0.91)
	26–35	12	4.63 (0.35)	4.30 (0.56)	4.47 (0.33)	4.80 (0.38)

Factor	Group	n	Generative AI Capabilities	AI-Based Fraud Detection and Prevention	Deepfake Financial Fraud Prevention	Data Privacy and Security
	Above 35	14	3.56 (1.28)	3.70 (1.36)	3.56 (1.28)	4.20 (1.31)
Gender	Female	99	3.71 (0.74)	3.58 (0.81)	3.60 (0.80)	3.87 (0.93)
	Male	31	4.15 (0.99)	3.96 (1.04)	3.95 (1.01)	4.37 (0.98)
Education	Higher Secondary	16	3.42 (1.04)	3.40 (1.04)	3.15 (0.95)	3.45 (1.14)
	Undergraduate	96	3.88 (0.70)	3.70 (0.78)	3.74 (0.76)	4.02 (0.87)
	Postgraduate	18	3.81 (1.13)	3.77 (1.20)	3.81 (1.15)	4.31 (1.10)
Occupation	Student	93	3.69 (0.75)	3.58 (0.84)	3.60 (0.83)	3.84 (0.94)
	Working / Other	37	4.11 (0.93)	3.91 (0.95)	3.89 (0.93)	4.36 (0.92)
Usage frequency	Daily	60	3.87 (0.89)	3.74 (0.94)	3.81 (0.93)	4.04 (1.02)
	Several times a week	39	3.62 (0.90)	3.36 (0.90)	3.40 (0.89)	3.79 (1.01)
	Monthly or less	31	3.94 (0.51)	3.93 (0.61)	3.79 (0.61)	4.14 (0.75)

Note. Each cell shows the mean with the standard deviation in parentheses. N = 130.

Age group was significantly associated with differences in all four constructs: Generative AI Capabilities, $F(2, 127) = 7.62$, $p < .001$, $\eta^2 = .107$; AI-Based Fraud Detection and Prevention, $F(2, 127) = 3.59$, $p = .030$, $\eta^2 = .054$; Deepfake Financial Fraud Prevention, $F(2, 127) = 5.92$, $p = .003$, $\eta^2 = .085$; and Data Privacy and Security, $F(2, 127) = 5.83$, $p = .004$, $\eta^2 = .084$. These are small-to-medium effect sizes. Bonferroni-adjusted comparisons showed that respondents aged 26–35 scored higher than both other groups on Generative AI Capabilities ($p = .001$ against up to 25; $p = .002$ against above 35) and Deepfake Financial Fraud Prevention ($p = .003$ and $p = .019$), and higher than those up to 25 on AI-Based Fraud Detection and Prevention ($p = .025$) and Data Privacy and Security ($p = .004$). Only the age effect on Generative AI Capabilities remains significant at the Bonferroni-adjusted level of .0025, so the other three age effects should be treated as indicative.

Two cautions apply to the age results. The 26–35 group ($n = 12$) and the above-35 group ($n = 14$) are small, and the above-35 group is much more dispersed, with an SD of 1.28 for Generative AI Capabilities compared with 0.35 in the 26–35 group. Levene's test, run outside Excel, indicated unequal variances for Generative AI Capabilities, AI-Based Fraud Detection and Prevention and Deepfake Financial Fraud Prevention ($p = .043$, $p = .016$ and $p = .016$), and Data Privacy and Security was borderline ($p = .051$). Kruskal–Wallis tests, which do not assume equal variances, led to the same conclusion for all four constructs (all $p \leq .015$).

Male respondents scored higher than female respondents on all four constructs ($p = .009$ to $.047$; $\eta^2 = .030$ to $.052$). Respondents who were working or in other occupations scored higher than students on Generative AI Capabilities ($p = .009$), AI-Based Fraud Detection and Prevention ($p = .048$) and Data Privacy and Security ($p = .006$), but not significantly on Deepfake Financial Fraud Prevention ($p = .078$). For the three significant constructs, η^2 ranged from .030 to .058. These are small effects. None reaches the Bonferroni-adjusted threshold, and the male group ($n = 31$) and the working group ($n = 37$) are much smaller than the comparison groups, so these differences are exploratory.

Educational qualification was significantly associated with differences in Deepfake Financial Fraud Prevention, $F(2, 127) = 3.62$, $p = .030$, $\eta^2 = .054$, and on Data Privacy and Security, $F(2, 127) = 3.71$, $p = .027$, $\eta^2 = .055$, but not on Generative AI Capabilities ($p = .127$) or AI-Based Fraud Detection and Prevention ($p = .403$). In the pairwise comparisons, higher-secondary respondents scored lower than undergraduates on Deepfake Financial Fraud Prevention ($p = .032$) and lower than postgraduates on Data Privacy and Security ($p = .027$), and the higher-secondary group has only 16 respondents. Frequency of use was significantly associated with differences in AI-Based Fraud Detection and Prevention, $F(2, 127) = 4.19$, $p = .017$, $\eta^2 = .062$. Respondents who use digital financial services several times a week scored lowest, and the only significant pairwise difference was between them and respondents who use such services monthly or less ($p = .020$). The effect on Deepfake Financial Fraud Prevention was borderline ($p = .052$). The pattern does not rise or fall steadily with usage, and these effects are small and exploratory.

10.6 Linear regression: tests of H1, H2 and H3

Table 11. Simple linear regression results for H1, H2 and H3

Hyp.	Relationship	B	SE	95% CI of B	β	t	p	R ²	F(1, 128)
H1	Generative AI Capabilities → AI-Based Fraud Detection and Prevention	0.895	0.051	0.793–0.997	.838	17.38	< .001	.702	301.97
H2	AI-Based Fraud Detection and Prevention → Deepfake Financial Fraud Prevention	0.843	0.045	0.755–0.931	.858	18.93	< .001	.737	358.53
H3	Generative AI Capabilities → Deepfake Financial Fraud Prevention	0.893	0.049	0.797–0.989	.852	18.40	< .001	.726	338.74

Note. N = 130. B is the unstandardised coefficient and β the standardised coefficient. All models are significant at $p < .001$.

H1. Generative AI Capabilities significantly and positively predicted AI-Based Fraud Detection and Prevention ($B = 0.895$, $SE = 0.051$, $\beta = .838$, $t(128) = 17.38$, $p < .001$). The model explained 70.2% of the variance ($R^2 = .702$, adjusted $R^2 = .700$), $F(1, 128) = 301.97$, $p < .001$. A one-point higher Generative AI Capabilities score was associated with a 0.89-point higher AI-Based Fraud Detection and Prevention score. H_{01} is rejected and H_{11} is supported.

H2. AI-Based Fraud Detection and Prevention significantly and positively predicted Deepfake Financial Fraud Prevention ($B = 0.843$, $SE = 0.045$, $\beta = .858$, $t(128) = 18.93$, $p < .001$). The model explained 73.7% of the variance ($R^2 = .737$, adjusted $R^2 = .735$), $F(1, 128) = 358.53$, $p < .001$. A one-point higher AI-Based Fraud Detection and Prevention score was associated with a 0.84-point higher Deepfake Financial Fraud Prevention score. H_{02} is rejected and H_{12} is supported.

H3. Generative AI Capabilities significantly and positively predicted Deepfake Financial Fraud Prevention ($B = 0.893$, $SE = 0.049$, $\beta = .852$, $t(128) = 18.40$, $p < .001$). The model explained 72.6% of the variance ($R^2 = .726$, adjusted $R^2 = .724$), $F(1, 128) = 338.74$, $p < .001$. A one-point higher Generative AI Capabilities score was associated with a 0.89-point higher Deepfake Financial Fraud Prevention score. H_{03} is rejected and H_{13} is supported.

The regression assumptions were checked. The Durbin–Watson statistics (2.28, 1.96 and 2.01) show no problem with independence of residuals, and the Breusch–Pagan tests (all $p > 0.56$) show no evidence of unequal residual variance. Residuals for H1 were approximately normal (Shapiro–Wilk $p = .320$), whereas those for H2 and H3 departed from normality ($p < .001$), as is expected with a negatively skewed, upper-bounded Likert score. With 130 cases the estimates are reasonably robust to this, but the p -values should be read with that limitation in mind.

10.7 Moderation analysis: test of H4

Table 12. Hierarchical moderated regression with the interaction between each predictor and Data Privacy and Security

Relationship tested	Step 1 R ²	Step 2 R ²	Interaction B (SE)	B	t(126)	p	ΔR^2	F change (p)
Generative AI Capabilities × Data Privacy and Security → AI-Based Fraud Detection and Prevention	.715	.715	−0.012 (0.039)	−0.019	−0.30	.762	.0002	0.09 (.762)
AI-Based Fraud Detection and Prevention × Data Privacy and Security → Deepfake Financial Fraud Prevention	.779	.779	−0.018 (0.032)	−0.028	−0.54	.588	.0005	0.30 (.588)
Generative AI Capabilities × Data Privacy and Security → Deepfake Financial Fraud Prevention	.746	.746	0.006 (0.036)	.010	0.18	.857	.0001	0.03 (.857)

Note. N = 130. Predictors are mean-centred. Step 1 contains the predictor and Data Privacy and Security, and Step 2 adds their product term.

Table 13. Main effects in Step 1 of the moderation models, with mean-centred predictors

Outcome and predictor	B (SE)	β	p
Outcome: AI-Based Fraud Detection and Prevention			
Generative AI Capabilities	0.718 (0.089)	.672	< .001
Data Privacy and Security	0.184 (0.076)	.201	.018
Outcome: Deepfake Financial Fraud Prevention			
AI-Based Fraud Detection and Prevention	0.612 (0.063)	.623	< .001
Data Privacy and Security	0.280 (0.057)	.311	< .001
Outcome: Deepfake Financial Fraud Prevention			
Generative AI Capabilities	0.678 (0.083)	.646	< .001
Data Privacy and Security	0.224 (0.071)	.249	.002

Note. N = 130; df = 2, 127 for each Step 1 model.

None of the three interaction terms was statistically significant. The interaction of Generative AI Capabilities and Data Privacy and Security on AI-Based Fraud Detection and Prevention had $B = -0.012$, $p = .762$. The interaction of AI-Based Fraud Detection and Prevention and Data Privacy and Security on Deepfake Financial Fraud Prevention had $B = -0.018$, $p = .588$, and the interaction of Generative AI Capabilities and Data Privacy and Security on Deepfake Financial Fraud Prevention had $B = 0.006$, $p = .857$. Adding the interaction term changed R^2 by no more than .0005 in any model, so Data Privacy and Security did not change the strength of the relationships in the framework. H_{04} is not rejected, and H_{14} is not supported.

Data Privacy and Security was, however, an independent predictor in all three Step 1 models. In the Step 1 models it predicted Deepfake Financial Fraud Prevention alongside AI-Based Fraud Detection and Prevention ($B = 0.280$, $p < .001$) and alongside Generative AI Capabilities ($B = 0.224$, $p = .002$), and it predicted AI-Based Fraud Detection and Prevention alongside Generative AI Capabilities ($B = 0.184$, $p = .018$). The variance inflation factors in the interaction models were below 3.5, with a highest value of 3.43, so collinearity is moderate. With 130 cases, the interaction test has 80% power only for effects of about $f^2 \geq 0.06$, which lies between small and medium. A small moderating effect therefore cannot be ruled out, although the estimated interaction effects are close to zero.

10.8 Summary of hypothesis testing

Table 14. Summary of hypothesis testing

Code	Test and relationship	Key statistics	Decision
H1	Simple regression: Generative AI Capabilities $\rightarrow$ AI-Based Fraud Detection and Prevention	$B = 0.895$, $\beta = .838$, $t = 17.38$, $p < .001$, $R^2 = .702$	H_{01} rejected; H_{11} supported
H2	Simple regression: AI-Based Fraud Detection and Prevention $\rightarrow$ Deepfake Financial Fraud Prevention	$B = 0.843$, $\beta = .858$, $t = 18.93$, $p < .001$, $R^2 = .737$	H_{02} rejected; H_{12} supported
H3	Simple regression: Generative AI Capabilities $\rightarrow$ Deepfake Financial Fraud Prevention	$B = 0.893$, $\beta = .852$, $t = 18.40$, $p < .001$, $R^2 = .726$	H_{03} rejected; H_{13} supported
H4	Hierarchical moderated regression: interaction with Data Privacy and Security in three relationships	Interaction $p = .762$, $.588$, $.857$; $\Delta R^2 \leq .0005$	H_{04} not rejected; H_{14} not supported

10.9 Supplementary analysis of the mediating pathway

The conceptual framework identifies AI-Based Fraud Detection and Prevention as a mediating variable, but the final hypotheses, H1 to H4, do not include a separate mediation hypothesis, and none has been added. The results below are a supplementary description of the mediating pathway shown in the framework and are not a hypothesis test.

Table 15. Supplementary multiple regression of Deepfake Financial Fraud Prevention on Generative AI Capabilities and AI-Based Fraud Detection and Prevention

Predictor	B	SE	β	t	p
Constant	0.150	0.165		0.91	.365
Generative AI Capabilities	0.467	0.077	.445	6.06	< .001
AI-Based Fraud Detection and Prevention	0.477	0.072	.485	6.61	< .001

Note. N = 130. $R^2 = .796$, adjusted $R^2 = .793$, $F(2, 127) = 247.62$, $p < .001$. VIF = 3.36 for each predictor.

When both predictors were entered together, each remained significant, and the model explained 79.6% of the variance in Deepfake Financial Fraud Prevention. The coefficient of Generative AI Capabilities fell from 0.893 in H3, without the mediating variable, to 0.467. The indirect effect through AI-Based Fraud Detection and Prevention was 0.427 (Sobel $Z = 6.18$, $p < .001$), with a bootstrap 95% confidence interval, run outside Excel, of 0.298 to 0.563. This is about 48% of the total association. This pattern is consistent with the mediating role shown in the framework, in which Generative AI Capabilities are related to Deepfake Financial Fraud Prevention both directly and through AI-Based Fraud Detection and Prevention. Because the data are cross-sectional and perception-based, this describes an association pattern and does not prove a causal process. Treating mediation as a formal hypothesis would require adding it to the research design separately, which has not been done here.

11. Discussion

The results support the direction of the three relationships proposed in the framework, but not a moderating role for Data Privacy and Security. This section compares the findings with earlier research and considers how far they can be interpreted.

Generative AI Capabilities and AI-Based Fraud Detection and Prevention

Respondents who rated Generative AI capabilities highly also rated AI-based fraud detection and prevention highly, and the relationship was strong ($\beta = .838$, $R^2 = .702$). This agrees with technical studies reporting that generative methods improve the detection of unusual or novel fraud patterns and help with imbalanced data (Kumar, 2025; Dixit, 2024; Shan et al., 2026), that synthetic data can strengthen identity-fraud detection (Igba et al., 2025), and that large language models combined with other methods improve detection performance (Hacini et al., 2025). Those studies measured detection performance, whereas this study records perceptions, so the agreement lies in the direction of the relationship and not in its size. Respondents who think well of what Generative AI can do also tend to think well of AI-based detection systems.

AI-Based Fraud Detection and Prevention for Deepfake Financial Fraud Prevention

AI-based fraud detection and prevention showed the strongest statistical association with perceived deepfake financial fraud prevention ($\beta = .858$, $R^2 = .737$). Multimodal, real-time and layered detection approaches are reported to perform well against deepfake-driven identity abuse, Video-KYC fraud and voice cloning (Amaresam, 2024; Rath, 2026; Rahat et al., 2026; Rawat et al., 2026; Gokul et al., 2026; Jayakannan, 2025), and Shan (2025) reports that AI and machine learning techniques can outperform traditional rule-based systems. Respondents who rated AI-based identity verification, risk scoring and real-time monitoring favourably also tended to believe that deepfake financial fraud can be prevented, which follows the logic of the framework.

Generative AI Capabilities and Deepfake Financial Fraud Prevention

Generative AI capabilities were also related to perceived deepfake financial fraud prevention when considered on their own ($\beta = .852$, $R^2 = .726$), and in the supplementary model this direct association remained significant after AI-based fraud detection and prevention was included ($\beta = .445$). Igba et al. (2025) and Rath (2026) describe capabilities such as synthetic data generation and multimodal, explainable detection that bear directly on deepfake-related fraud. Respondents therefore appear to see Generative AI as relevant to deepfake prevention both directly and through AI-based detection systems. The very high correlations among the three main constructs ($r = .838$ to $.858$) mean, however, that part of this overlap may reflect a general favourable attitude towards AI and not separate judgements about each construct.

Data Privacy and Security

Data Privacy and Security had the highest mean of the four constructs (3.99) and correlated strongly with the others, yet none of the three interaction terms was significant, so H_{04} was not rejected. The variable was nevertheless positively related to perceived deepfake financial fraud prevention when entered alongside the predictors. Earlier studies repeatedly identify privacy, explainability and regulatory compliance as conditions for deploying AI against fraud (Amaresam, 2024; Kumar, 2025; Rawat et al., 2026; Senevirathna & Sumanathilaka, 2025; Delva Benavides et al., 2026; Marwick et al., 2026; Zeng et al., 2026). Respondents clearly value privacy and security, but in this sample it works as a supporting condition that goes together with favourable views of AI-based prevention rather than as a factor that strengthens or weakens the Generative AI or detection relationships. This does not show that privacy and security are unimportant. With 130 responses, small moderating effects could not be detected, and the construct was measured through privacy, security and compliance items only.

Differences across respondents

Perceptions differed significantly by age group, and to a smaller extent by education, gender and occupation, with respondents aged 26–35 the most favourable. Most of these differences are exploratory because the groups are small and unequal, and only the age-group effect for Generative AI Capabilities survived the Bonferroni adjustment. Adegoke and Adegoke (2026) also examined demographic factors such as age, gender, education and employment among digital finance users, although they looked at fraud exposure and not at perceptions of prevention. Awareness of and exposure to AI-enabled financial services may likewise differ between age and occupational groups, which would be worth testing in a more balanced sample. Frequency of use showed no consistent pattern.

Overall, all findings describe respondents' perceptions and assessments. They do not show that Generative AI actually reduces deepfake financial fraud, and the cross-sectional design does not allow causal conclusions.

12. Implications

12.1 Theoretical implications

The study provides primary questionnaire-based empirical evidence, based on respondents' perceptions, for an integrated framework that links Generative AI capabilities, AI-based fraud detection and prevention, and deepfake financial fraud prevention. The reviewed literature is mainly technical, conceptual or policy-based, as the review in Section 8 shows, so a test of the relationships based on respondents' perceptions adds a different kind of evidence. Data Privacy and Security did not moderate the relationships but was related to perceived deepfake financial fraud prevention. Its role in the framework may therefore be better described as a supporting condition than as a boundary condition, a point that needs to be tested with larger samples and a fuller measure of the moderating variable.

12.2 Practical implications

Integrating Generative AI with detection systems. Respondents linked Generative AI capabilities with AI-based detection and with deepfake prevention. Banks and FinTech firms may therefore benefit from embedding Generative AI in identity verification, risk scoring and real-time monitoring, with human review where needed (Amaresam, 2024; Rawat et al., 2026).

Privacy and security. Data Privacy and Security received the highest ratings, so institutions that communicate strong data protection and regulatory compliance may strengthen confidence in AI-based systems (Senevirathna & Sumanathilaka, 2025; Rawat et al., 2026).

Targeted awareness and training. Perceptions differed by age group and, less strongly, by education, gender and occupation. Awareness programmes for customers and employees could be adapted to different groups and should address the verification and authorisation gaps highlighted in the literature (Delva Benavides et al., 2026; Adegoke & Adegoke, 2026).

Coordinated governance. Policymakers and industry bodies can take into account how strongly respondents emphasised data protection when designing standards for authentication, traceability and accountability (Delva Benavides et al., 2026; Marwick et al., 2026; Kurshan et al., 2024).

13. Limitations and Future Research

The findings should be read in light of the following limitations.

Perception-based data. The questionnaire records agreement with statements. It does not measure actual fraud incidents, financial losses, detection accuracy, false-positive rates or response times, even though some of these appear as indicators in the conceptual framework.

Sample composition and sampling. The respondents are mainly young students: 71.5% are students, 80.0% are aged 25 or below, including 6.2% below 18, and 76.2% are female. The study used non-probability convenience sampling, so the results describe the perceptions of this sample and cannot be generalised to FinTech users as a whole. Several subgroups are small, for example 12 respondents aged 26–35 and 14 above 35.

Construct overlap and validity. The constructs are highly correlated, and the Deepfake Financial Fraud Prevention items are worded around Generative AI, which overlaps with the independent variable. The discriminant validity of the constructs was not tested and should be examined in future research.

Measurement of the moderating variable. In the framework, Data Privacy and Security includes scalability and cost, model accuracy and bias, explainability and transparency, and talent and skill gaps. The questionnaire measures the variable through privacy, security and compliance statements only, so the other dimensions were not tested.

Design and statistical analysis. The cross-sectional, single-source design does not allow causal conclusions. Likert scores were analysed as continuous data in Excel, scores are skewed towards agreement, and the residuals for H2 and H3 were not normally distributed. Many ANOVA and chi-square tests were run, so findings other than the age-group effect on Generative AI Capabilities are exploratory. Dividing scores into two levels for the chi-square tests also loses information.

Statistical power. With 130 responses, the moderation tests can detect only small-to-medium or larger effects (f^2 of about .06 or more), so a smaller moderating effect cannot be excluded.

Future research could collect questionnaire data from a larger and more balanced sample, including working professionals and other FinTech users, and could add objective indicators of fraud prevention to complement perceptions. Confirmatory factor analysis or PLS-SEM could be used to test discriminant validity and to estimate direct, indirect and moderating effects simultaneously with bootstrapped confidence intervals. Studies could also measure the full set of moderating dimensions shown in the framework, namely explainability, bias, cost and scalability, and talent gaps, and compare groups such as age, occupation and sector using samples large enough to support such comparisons.

14. Conclusion

This study set out to examine how Generative AI capabilities relate to AI-based fraud detection and prevention and to deepfake financial fraud prevention in the FinTech ecosystem, and whether Data Privacy and Security alters those relationships. The integrated conceptual framework used here links Generative AI Capabilities to AI-Based Fraud Detection and Prevention, and the latter to Deepfake Financial Fraud Prevention. It also includes a direct relationship between Generative AI Capabilities and Deepfake Financial Fraud Prevention and treats Data Privacy and Security as a moderating, or contextual, variable.

Based on 130 questionnaire responses, the three core relationships were supported. Respondents who rated Generative AI capabilities highly also rated AI-based fraud detection and prevention highly ($H1$; $\beta = .838$, $R^2 = .702$), and respondents who rated AI-based fraud detection and prevention highly were more likely to perceive deepfake financial fraud as preventable ($H2$; $\beta = .858$, $R^2 = .737$). Generative AI capabilities were also directly related to perceived deepfake financial fraud prevention ($H3$; $\beta = .852$, $R^2 = .726$). The supplementary analysis, which is not a hypothesis test, pointed the same way: the association between Generative AI capabilities and perceived deepfake prevention remained significant when AI-based fraud detection and prevention was included, while a substantial part of it ran through that variable. Respondents therefore appear to regard Generative AI as relevant to deepfake prevention both on its own and as part of AI-based detection systems.

The moderating role proposed for Data Privacy and Security was not supported. None of the three interaction terms was significant, so H_{04} was not rejected and H_{14} was not supported. This does not make privacy and security unimportant. Data Privacy and Security received the highest ratings of the four constructs and was positively related to perceived deepfake financial fraud prevention in every model in which it was entered. In this sample it is better understood as a supporting condition that accompanies favourable views of AI-based prevention than as a factor that strengthens or weakens the other relationships. With 130 responses, however, only small-to-medium or larger moderating effects could have been detected, so a smaller effect cannot be ruled out.

For the FinTech ecosystem, the findings suggest that Generative AI is most likely to be seen as useful when it is built into AI-based detection and prevention systems, for example in identity verification, risk scoring and real-time monitoring, and not treated as a stand-alone tool. Institutions that wish to build confidence in such systems should communicate their data protection and regulatory compliance practices clearly, since respondents attached high importance to them. Perceptions also varied by age group and, to a lesser extent, by education, gender and occupation, which indicates that awareness and training programmes may need to be adapted to different groups of customers and employees.

The findings must be interpreted within the limits of the study. The questionnaire measured perceptions and assessments, and not actual fraud incidents, financial losses, detection accuracy or response times, so the results describe what respondents perceive and do not show that Generative AI reduces deepfake financial fraud in practice. The sample was mainly young and student-based and was drawn by convenience sampling, the constructs were highly correlated and their discriminant validity was not tested, the design was cross-sectional, and the moderating variable was measured through privacy, security and compliance statements only. The relationships reported are associations.

Future research should therefore build on these results with larger and more balanced samples that include working professionals and other FinTech users, add objective indicators of fraud prevention to complement perceptions, and use confirmatory factor analysis or PLS-SEM to test discriminant validity and to estimate direct, indirect and moderating effects together. Measuring the full set of privacy and security dimensions shown in the framework would allow a fuller test of the moderating role. As Generative AI continues to change both the methods of financial fraud and the tools used against it, evidence on how stakeholders view the technology on which fraud prevention increasingly depends, and on the part played by data privacy and security, will remain important to institutions, regulators and researchers.

References

1. Shan, W. (2025). AI-powered fraud detection in banking: Innovations, challenges and preventive strategies [Master's thesis, Saint Mary's University].
2. Rath, M. K. (2026). Adversarial resilient and explainable AI framework for deepfake-aware fraud detection in financial systems. *International Journal of Computer Information Systems and Industrial Management Applications*, 18(8s), 1072–1085. <https://doi.org/10.70917/ijcisim-2026-3363>

3. Rahat, Y. O., Islam, M. K., & Rabbani, S. F. (2026). Machine learning for identifying deepfake-driven identity abuse, authentication evasion, and customer impersonation in U.S. banking. *Frontiers in Computer Science and Artificial Intelligence*, 5(4), 54–67. <https://doi.org/10.32996/fcsai.2026.4.3.7x>
4. Amaresam, R. K. (2024). Deepfake detection and AI's role in preventing digital fraud. *International Journal of Research and Applied Innovations*, 7(4), 11096–11107. <https://doi.org/10.15662/IJRAI.2024.0704011>
5. Marwick, A. E., Schiffrin, A., & Williams, K. (2026). Governing the scam ecosystem: Policy responses to generative AI-enabled deepfake financial fraud [Preprint]. SSRN. <https://ssrn.com/abstract=6866865>
6. Kurshan, E., Mehta, D., & Balch, T. (2024). AI versus AI in financial crimes & detection: GenAI crime waves to co-evolutionary AI. In *Proceedings of the 5th ACM International Conference on AI in Finance* (pp. 745–751). Association for Computing Machinery. <https://doi.org/10.1145/3677052.3698655>
7. Delva Benavides, J. E., Leos Navarro, J. A., & García Hernández, A. P. (2026). Deepfakes in onboarding, KYC, and financial fraud: Authenticity standards and liability framework for digital banks and FinTech. *Journal of FinTech and Sustainable Finance*, 2, 1–9. <https://doi.org/10.31875/2755-8398.2026.02.01>
8. Zeng, Q., Zhao, Z., Yang, Y., Zhu, Y., Liu, F., Bi, Z., Wynn, M. T. K., Choo, K.-K. R., & Chen, H. (2026). When AI meets Wall Street: A survey on trustworthy AI in fintech (arXiv:2605.30650). arXiv. <https://arxiv.org/abs/2605.30650>
9. Adegoke, K. R., & Adegoke, T. B. (2026). AI-enabled fraudulent schemes and their effects on consumer trust and digital financial adoption in Nigeria. *SSR Journal of Multidisciplinary*, 3(1), 20–36. <https://doi.org/10.5281/zenodo.18228379>
10. Kumar, S. N. P. (2025). Fraud detection in banking using generative AI. *Sarcouncil Journal of Engineering and Computer Sciences*, 4(11), 133–145. <https://doi.org/10.5281/zenodo.17634095>
11. Dixit, S. (2024). Advanced generative AI models for fraud detection and prevention in FinTech: Leveraging deep learning and adversarial networks for real-time anomaly detection in financial transactions [Preprint]. TechRxiv. <https://doi.org/10.36227/techrxiv.172978266.60563345/v1>
12. Shan, K., Wang, J., Wang, Q., Chen, G., & Mansoor, A. (2026). Leveraging generative AI for financial fraud detection in the platform economy: A GAN-based data augmentation method. *Humanities and Social Sciences Communications*. Advance online publication. <https://doi.org/10.1057/s41599-026-07552-x>
13. Senevirathna, L., & Sumanathilaka, D. (2025). Efficient financial fraud detection on mobile devices using lightweight large language models. In *Proceedings of Recent Advances in Natural Language Processing* (pp. 1090–1098). <https://doi.org/10.26615/978-954-452-098-4-126>
14. Hacini, A. D., Benabdelouahad, M., Abassi, I., Houhou, S., Boulmerka, A., & Farhi, N. (2025). LLM-assisted financial fraud detection with reinforcement learning. *Algorithms*, 18(12), Article 792. <https://doi.org/10.3390/a18120792>
15. Rawat, R., Dibouliya, A., Chaturvedi, N., Rawat, A., Rawat, H., & Dangi, C. S. (2026). A data analytics based federated biometrics for deepfake fraud detection in financial multimedia systems. *Discover Computing*, 29, Article 215. <https://doi.org/10.1007/s10791-026-10073-5>
16. Jayakannan, S. M. (2025). Securing voice-based financial authentication in the era of AI voice cloning: Challenges, vulnerabilities, and counter-measures. *Journal of Computer Science and Technology Studies*, 7(4), 515–520. <https://doi.org/10.32996/jcsts.2025.7.4.60>
17. Gokul, P., Janarthan, R., Makeswaran, M. A., Karuppasamy, K., Thenmalar, R., & Jayaraman, S. (2026). Deepfake voice based scam detection in banking calls using AI and ML. *International Journal of Scientific Research and Engineering Development*, 9(2), 2292–2298. <https://www.ijrsred.com/volume9/issue2/IJSRED-V9I2P337.pdf>
18. Igba, E., Olarinoye, H. S., Nwakaego, V. E., Sehemba, D. B., Oluhaiyero, Y. S., & Okika, N. (2025). Synthetic data generation using generative AI to combat identity fraud and enhance global financial cybersecurity frameworks. *International Journal of Scientific Research and Modern Technology*, 4(2), 1–19. <https://doi.org/10.5281/zenodo.14928919>