

The double-edged sword of artificial intelligence in social commerce: how convenience, AI-enabled deception risk, and anti-fraud safeguards shape vulnerability, trust, and purchase intention

Valentino Aris^{1*}, Idayanti Nursyamsi², Arini Lestari Aris³, Muhammad Ashdaq³

¹Department of Business and Entrepreneur, Faculty of Economics and Business, Universitas Negeri Makassar, Indonesia

²Department of Management, Faculty of Economics and Business, Universitas Hasanuddin, Indonesia

³Department of Management, Faculty of Economics, Universitas Andi Djemma, Indonesia

Abstract

The rapid growth of AI-enabled social commerce creates both functional benefits and emerging risks for consumers, making it important to understand how AI-related perceptions are associated with purchase intention. This study examines the relationships among perceived AI convenience, AI-enabled deception risk, perceived platform anti-fraud safeguards, perceived vulnerability to AI fraud, customer trust, and purchase intention. Using a quantitative explanatory design, data were collected from 720 Indonesian social commerce users through non-probability purposive and snowball sampling and analysed using Partial Least Squares Structural Equation Modelling (PLS-SEM). The findings show that perceived AI convenience and perceived platform anti-fraud safeguards were associated with lower perceived vulnerability to AI fraud, stronger customer trust, and higher purchase intention. In contrast, AI-enabled deception risk was associated with greater perceived vulnerability, weaker customer trust, and lower purchase intention. Significant indirect relationships were also observed through perceived vulnerability to AI fraud and customer trust, supporting their roles as two distinct parallel psychological mechanisms linking AI-related perceptions with purchase intention. The study contributes to digital-commerce research by integrating AI-enabled convenience, deception risk, and institutional safeguards within a unified risk-trust framework and by distinguishing consumers' personal vulnerability from confidence in the platform. Practically, social commerce platforms should combine AI-enabled convenience with visible anti-fraud safeguards, transparent AI practices, effective reporting mechanisms, and trust-building strategies to support more secure and confident consumer decision-making.

Keywords:

algorithmic persuasion; digital consumer protection; institutional assurance; platform governance; threat appraisal.

JEL Code: D18; D83; D91

Received November 17, 2025; Received in revised form August 19, 2026;
Accepted August 29, 2026; Available online October 23, 2026

*Corresponding author

Email: valentino.aris@unm.ac.id



To cite this document:

Aris, V., Nursyamsi, I., Aris, A. L., & Ashdaq, M. (2026). The double-edged sword of artificial intelligence in social commerce: how convenience, AI-enabled deception risk, and anti-fraud safeguards shape vulnerability, trust, and purchase intention. *BISMA (Bisnis dan Manajemen)*, 19(1), 1–27. <https://doi.org/10.26740/bisma/v19n1.p1-27>

Introduction

Social commerce integrates product discovery, social interaction, and purchasing through consumer reviews, recommendations, creator content, and community engagement (Hajli, 2015; Hajli et al., 2017). Within these environments, AI-based recommender systems and personalised suggestions facilitate product discovery and reduce information-search effort, supporting more convenient shopping experiences (Valencia-Arias et al., 2024; Yin et al., 2025). Trust and perceived risk also shape consumers' willingness to purchase, making both central to understanding social commerce decisions (Senali et al., 2024; Wang et al., 2022).

Alongside these benefits, AI can generate convincing fake reviews and other deceptive content that complicate consumers' assessments of commercial information (Salminen et al., 2022; Schmitt & Flechais, 2024). Generative AI further supports impersonation, phishing, and social engineering, extending its implications beyond shopping efficiency to consumers' exposure to fraud (Schmitt & Flechais, 2024). Consumers' evaluations of AI-enabled commerce therefore require attention to functional benefits alongside vulnerability and trust, which existing research connects to digital shopping experiences and purchasing decisions (Valencia-Arias et al., 2024).

Prior studies have examined AI recommendations and consumer responses (Valencia-Arias et al., 2024; Yin et al., 2025), trust and purchase intention in social commerce (Hajli et al., 2017), and AI-enabled deception and fraud-related vulnerability (Qu et al., 2024; Schmitt & Flechais, 2024). Research on structural assurance additionally explains how platform protection mechanisms relate to trust and purchase intention (Saxena & Thakur, 2024). However, these streams leave insufficiently explained how AI convenience, deception risk, and perceived platform safeguards jointly relate to purchase intention through personal vulnerability and platform trust as distinct psychological mechanisms (Valencia-Arias et al., 2024; Schmitt & Flechais, 2024; Wagner et al., 2023; Saxena & Thakur, 2024).

This study aims to examine the direct and indirect relationships of perceived AI convenience, AI-enabled deception risk, and perceived platform anti-fraud

safeguards with purchase intention through perceived vulnerability to AI fraud and customer trust among Indonesian social commerce users.

A quantitative cross-sectional survey was conducted between August and September 2025, yielding 720 eligible, consenting respondents recruited through purposive and snowball sampling. Participants had recent purchasing experience involving social commerce and AI-enabled features. Data were collected using a seven-point Likert-scale questionnaire and analysed using partial least squares structural equation modelling in SmartPLS 4. The analysis assessed the measurement and structural models and used bootstrapping to examine direct relationships and specific indirect relationships through vulnerability and trust as parallel mediators.

The study contributes an integrated explanation of purchase intention that connects AI's functional benefits and deceptive potential with perceived platform protection. Drawing on Protection Motivation Theory and institution-based trust and structural assurance perspectives, it distinguishes consumers' sense of personal exposure to AI fraud from their confidence in the platform. This distinction clarifies the complementary roles of threat-related perceptions and trust in AI-enabled purchasing decisions. The contribution is bounded to consumer perceptions within Indonesian social and AI-enabled commerce rather than objective platform security or marketplace transactions generally.

Literature review

Theoretical foundation

Protection Motivation Theory (PMT) explains consumers' evaluations of threats and protective responses in AI-enabled social commerce. Rogers (1975, 1983) distinguished threat appraisal from coping appraisal, which cybersecurity research applies to digital threats and cyber fraud (Bekkers et al., 2023; Hassan et al., 2024). Threat probability concerns an event's likelihood, susceptibility concerns personal exposure, severity concerns anticipated consequences, and coping efficacy concerns protective effectiveness. This study conceptualises perceived vulnerability to AI fraud as a broader subjective sense of personal exposure, related to but distinct from these appraisals.

Institution-based trust and structural assurance complement PMT by explaining confidence in platform protection. Institutional and technological assurances signal credible protection and can strengthen trust and purchase intention (McKnight et al., 2002; Saxena & Thakur, 2024). Accordingly, perceived safeguards concern external protection, trust concerns platform competence, integrity, and reliability, and vulnerability concerns personal exposure to harm (Wagner et al., 2023). Purchase intention captures willingness or plans to purchase and precedes actual behaviour (Fishbein & Ajzen, 1975; Pavlou, 2003). Together, these perspectives distinguish threat appraisal,

vulnerability, safeguards, trust, and purchase intention within an integrated framework.

Perceived AI convenience

Service convenience concerns purchasing time and effort, while online shopping convenience encompasses accessing, searching, evaluating, transacting, and obtaining products (Berry et al., 2002; Jiang et al., 2013). In AI recommendations, personalised feeds, and intelligent assistants support convenience by reducing information overload and simplifying decisions (Santy et al., 2024). Perceived AI convenience therefore denotes consumers' perceptions that platform AI reduces the effort required to find, evaluate, and purchase products. Online convenience can reduce effort and uncertainty while supporting perceptions of platform competence, trust, and purchase-related intentions (Jiang et al., 2013; Nurdianasari et al., 2025; Santy et al., 2024). These benefits underpin the following hypotheses.

H1a: Perceived AI convenience has a negative effect on perceived vulnerability to AI fraud.

H1b: Perceived AI convenience has a positive effect on customer trust.

H1c: Perceived AI convenience has a positive effect on purchase intention.

AI-Enabled deception risk

AI-enabled deception involves generating or amplifying misleading information through deepfakes, fabricated reviews, manipulated product information, and other synthetic content (Park et al., 2024; Williamson & Prybutok, 2024; Schmitt & Flechais, 2024). Here, AI-enabled deception risk denotes consumers' perceptions that AI technologies or content may mislead them during purchasing. Exposure to deceptive practices and awareness of technology-assisted fraud can heighten vulnerability and fear while weakening trust (Iwara, 2025; Qu et al., 2024; Shang et al., 2022). Fraud-related risk and misleading AI-generated information can also reduce trust and reliance on platform information when purchasing (Wang et al., 2022; Amos & Zhang, 2024; Salminen et al., 2022). Thus, the hypothesis formulated is as follows.

H2a: AI-enabled deception risk positively affects perceived vulnerability to AI fraud.

H2b: AI-enabled deception risk negatively affects customer trust.

H2c: AI-enabled deception risk negatively affects purchase intention.

Perceived platform anti-fraud safeguards

Perceived platform anti-fraud safeguards denote consumers' beliefs that platforms communicate and enforce protection against AI-enabled fraud through monitoring, verification, warnings, reporting, and redress. Security and protection mechanisms can reduce perceived risk, strengthen trust, and support digital

service intentions (Almaiah et al., 2023; Chung & Yu, 2021; Gupta & Hakhu, 2021). Transparent procedures, perceived security, and dispute resolution further reinforce confidence and repurchase intentions (Chung & Yu, 2021; Gupta & Hakhu, 2021). Therefore, the hypothesis can be stated as follows.

H3a: Perceived platform anti-fraud safeguards negatively affect perceived vulnerability to AI fraud.

H3b: Perceived platform anti-fraud safeguards positively affect customer trust.

H3c: Perceived platform anti-fraud safeguards positively affect purchase intention.

Perceived vulnerability to AI fraud

Perceived vulnerability denotes subjective personal exposure to harm from online threats, fraud, or information misuse (Debb & McClellan, 2021; Rejikumar et al., 2021). Here, it concerns exposure to AI-enabled fraud involving deepfakes, fake reviews, and synthetic endorsements. As distinguished above, this broader perception differs from threat probability, susceptibility, severity, and coping efficacy (Hassan et al., 2024). Greater vulnerability can increase uncertainty, weaken reliance on digital information, and discourage online purchasing (Wagner et al., 2023; Lo Presti & Maggiore, 2023; Nguyen et al., 2025). It is therefore proposed as a mediator linking AI convenience, deception risk, and platform safeguards to purchase intention:

H4a: Perceived vulnerability to AI fraud negatively affects purchase intention.

H4b: Perceived vulnerability to AI fraud mediates the relationship between AI-enabled deception risk and purchase intention.

H4c: Perceived vulnerability to AI fraud mediates the relationship between perceived platform anti-fraud safeguards and purchase intention.

H4d: Perceived vulnerability to AI fraud mediates the relationship between perceived AI convenience and purchase intention.

Customer trust

Customer trust denotes confidence in an online platform's competence, honesty, benevolence, and reliability under transactional uncertainty (Gefen, 2000; McKnight et al., 2002). This study focuses on trusting beliefs about platform attributes and responsible conduct, including data handling, rather than trusting intention, or willingness to depend on the platform. Such beliefs can strengthen purchase intention by increasing confidence in platform information, recommendations, and transactions (Pavlou, 2003; Wang et al., 2022). Convenience, usefulness, security, and protection can strengthen trust, whereas risk and uncertainty can weaken it, supporting its mediating role (Kim et al., 2008; Almaiah et al., 2023; Gupta & Hakhu, 2021).

H5a: Customer trust positively affects purchase intention.

H5b: Customer trust mediates the relationship between perceived AI convenience and purchase intention.

H5c: Customer trust mediates the relationship between AI-enabled deception risk and purchase intention.

H5d: Customer trust mediates the relationship between perceived platform anti-fraud safeguards and purchase intention.

Purchase intention

Purchase intention denotes willingness or plans to purchase and is a proximal antecedent of purchasing behaviour (Fishbein & Ajzen, 1975; Spears & Singh, 2004; Pavlou, 2003). Here, it concerns future purchases following engagement with AI-enabled social commerce. Convenience, personalisation, and trust can strengthen purchase intention by reducing effort and increasing confidence (Sintia et al., 2023; Wang et al., 2022). Conversely, fraud risk, vulnerability, and uncertainty can discourage purchases, while visible safeguards support trust and transaction intentions (Debb & McClellan, 2021; Lo Presti & Maggiore, 2023; Handoyo, 2024; Senali et al., 2024). Purchase intention is therefore the model's principal behavioural outcome, as shown in Figure 1.

Research method

Research design

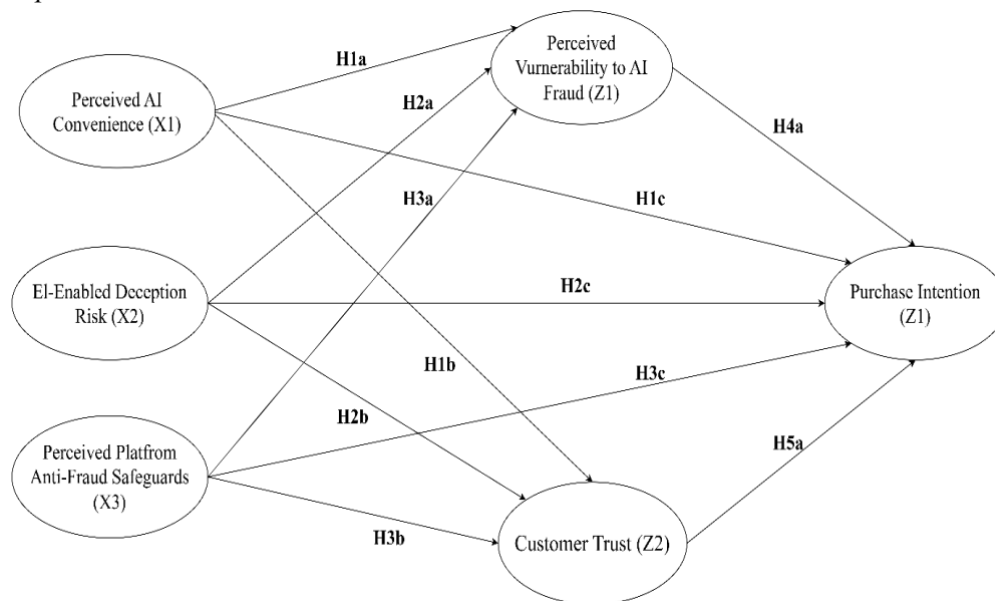
This study employed a quantitative explanatory design using a cross-sectional survey to examine relationships among six latent constructs: Perceived AI Convenience, AI-Enabled Deception Risk, Perceived Platform Anti-Fraud Safards, Perceived Vulnerability to AI Fraud, Customer Trust, and Purchase Intention. The proposed model positions perceived vulnerability and customer trust as parallel mediators, as illustrated in Figure 1. Given the cross-sectional design, the analysis examined associations among consumer perceptions and purchase intention without establishing causality.

Population and sampling

The target population comprised Indonesian consumers who had purchased through social-commerce-related features within the preceding six months and interacted with AI functionalities such as personalised recommendations, algorithmic feeds, or automated product suggestions. Eligible experiences included TikTok Shop and Instagram Shop transactions, alongside purchases through Shopee, Tokopedia, and Lazada involving social, live-commerce, recommendation, or other AI-enabled features. Conventional marketplace transactions alone were insufficient for inclusion. Purposive sampling identified eligible consumers, while snowball sampling extended recruitment through participants' networks. Of 760 submissions, 40 were excluded because respondents declined consent, leaving 720 eligible, consenting participants for analysis. Respondent characteristics are reported in Appendix 1.

Figure 1.

Proposed research model



Note: The indirect effects are assessed through six specific mediation paths: $X2 \rightarrow Z1 \rightarrow Y1$ (H4b), $X3 \rightarrow Z1 \rightarrow Y1$ (H4c), $X1 \rightarrow Z1 \rightarrow Y1$ (H4d), $X1 \rightarrow Z2 \rightarrow Y1$ (H5b), $X2 \rightarrow Z2 \rightarrow Y1$ (H5c), and $X3 \rightarrow Z2 \rightarrow Y1$ (H5d)

Source: Authors' Work (2026)

Measurement development and refinement

The six constructs were operationalised using multi-item reflective measures informed by established theoretical and empirical literature. The initial questionnaire contained 36 indicators measured on a seven-point Likert scale, ranging from 1 ("strongly disagree") to 7 ("strongly agree"). The instrument combined contextual adaptations, contextual reformulations, and contextually developed indicators. AI-Enabled Deception Risk and Perceived Platform Anti-Fraud Safeguards required greater reformulation to capture AI-specific risks and protective mechanisms.

An item-level conceptual reassessment identified five indicators whose content more closely aligned with other conceptual domains. X3_6 reflected transactional safety rather than platform safeguards; Z1_3 captured fraud-recognition self-efficacy rather than vulnerability; Z1_6 concerned the severity of potential consequences rather than personal exposure; Z2_4 reflected trusting intention rather than trusting beliefs; and Y1_4 measured recommendation or word-of-mouth intention rather than personal purchase intention. Their exclusion was based on conceptual correspondence and construct distinctiveness rather than statistical performance alone. The refined instrument retained 31 indicators. All constructs were specified as reflective because their indicators represented manifestations of underlying perceptions. The PLS-SEM model was subsequently re-estimated, and its measurement properties were reassessed.

Appendix 2 presents the retained indicators, conceptual foundations, sources, and adaptation types; Appendix 5 documents the excluded indicators and reasons for exclusion.

Data collection

Data were collected through Google Forms between August and September 2025. An informed consent statement appeared at the beginning of the questionnaire, and recorded consent status determined inclusion. Of 760 submissions, 40 were excluded before statistical analysis because respondents declined consent. The remaining 720 submissions from consenting respondents who met the eligibility criteria constituted the final analytical sample.

Data analysis

Data were analysed using Partial Least Squares Structural Equation Modelling (PLS-SEM) in SmartPLS 4 to examine the proposed relationships and parallel mediation through perceived vulnerability and customer trust. Analysis followed two stages. First, the measurement model containing 31 retained indicators was assessed for indicator reliability, internal consistency reliability, convergent validity, and discriminant validity. Discriminant validity was evaluated using the Fornell–Larcker criterion and the heterotrait–monotrait ratio of correlations (HTMT). Second, the structural model was evaluated for direct relationships, specific indirect effects, collinearity, explanatory power, effect sizes, and overall model fit. Bootstrapping assessed the statistical significance and confidence intervals of direct and specific indirect effects. Because all focal variables were measured through the same questionnaire, potential common method bias was additionally examined using full-collinearity VIF. These values were interpreted alongside the broader measurement evidence as diagnostic indicators rather than a definitive assessment of common method bias.

Results

Respondent characteristics

The sample comprised 720 respondents, predominantly female (72%) and aged 18–25 (63.33%), within an overall age range of 18–47 years. Students accounted for 40%, followed by private employees (35%), public servants or state-owned enterprise employees (15%), business owners (6.94%), and other occupations (3.06%). Educational attainment comprised high school (45.69%), bachelor's (31.94%), master's (13.19%), and doctoral degrees (9.17%) (Appendix 1). TikTok Shop was the most frequently used platform (35%), followed by Shopee (25%), Tokopedia and Instagram Shop (15% each), and Lazada (10%).

Measurement model

Indicator loadings (0.824–0.866) and AVE values (0.704–0.737) exceeded the respective thresholds of 0.70 and 0.50, supporting convergent validity (Appendix 2). Internal consistency was satisfactory, with Cronbach's alpha ranging from 0.881 to 0.918, rho_A from 0.881 to 0.919, and composite reliability (rho_C) from 0.918 to 0.936. All constructs met the Fornell–Larcker criterion, with square roots of AVE exceeding their inter-construct correlations (Appendix 3). HTMT values ranged from 0.038 to 0.892, remaining below 0.90 (Appendix 4). However, the HTMT between Customer Trust and Purchase Intention (0.892) approached this threshold, warranting caution when interpreting their distinctiveness.

Structural model

Bootstrapping assessed direct and specific indirect relationships, reported alongside total effects in Tables 2–4. Model fit indices were SRMR = 0.034, NFI = 0.935, d_ULS = 0.575, and d_G = 0.257. These were interpreted descriptively, particularly d_ULS and d_G, for which bootstrapped reference values were unavailable. Full-collinearity VIF values ranged from 1.710 to 4.134 (Appendix 6). Customer Trust (3.894) and Purchase Intention (4.134) exceeded the conservative criterion of 3.3, although all values remained below 5.0. Thus, severe collinearity was not indicated, but potential common-method influence could not be excluded. The model explained 56.4% of the variance in Perceived Vulnerability to AI Fraud, 66.5% in Customer Trust, and 75.8% in Purchase Intention. For vulnerability, effect sizes were large for deception risk ($f^2 = 0.843$), medium for safeguards (0.271), and small for convenience (0.117). All three predictors showed large effects on trust ($f^2 = 0.494$ –0.741). For purchase intention, trust had a medium effect (0.279), deception risk (0.127) and vulnerability (0.085) had small effects, and convenience (0.017) and safeguards (0.018) had negligible direct effects. Despite their statistical significance, the latter direct relationships had limited practical magnitude and were accompanied by significant indirect relationships, particularly through trust.

Table 1 supports all hypothesised direct relationships (all $p < 0.001$). AI convenience and platform safeguards were associated with lower vulnerability, greater trust, and higher purchase intention, whereas deception risk was associated with the opposite pattern. Deception risk had the strongest association with vulnerability ($\beta = 0.607$), whereas convenience had the strongest association with trust ($\beta = 0.498$). Trust was positively associated with purchase intention ($\beta = 0.453$), whereas deception risk ($\beta = -0.267$) and vulnerability ($\beta = -0.219$) were negatively associated. The direct associations of convenience and safeguards with purchase intention were comparatively small (Both $\beta = 0.086$; $f^2 = 0.017$ and 0.018, respectively).

Table 1.

Direct effects and hypothesis testing

Hypothesis	Relationship	β	t-value	p-value	95% BC CI	f^2	Decision
H1a	X1 $\rightarrow$ Z1	-0.226	9.360	<0.001	[-0.272, -0.178]	0.117	Supported
H1b	X1 $\rightarrow$ Z2	0.498	21.926	<0.001	[0.454, 0.542]	0.741	Supported
H1c	X1 $\rightarrow$ Y1	0.086	3.397	<0.001	[0.036, 0.135]	0.017	Supported
H2a	X2 $\rightarrow$ Z1	0.607	26.272	<0.001	[0.559, 0.650]	0.843	Supported
H2b	X2 $\rightarrow$ Z2	-0.471	21.113	<0.001	[-0.514, -0.425]	0.660	Supported
H2c	X2 $\rightarrow$ Y1	-0.267	9.515	<0.001	[-0.322, -0.213]	0.127	Supported
H3a	X3 $\rightarrow$ Z1	-0.344	14.091	<0.001	[-0.393, -0.296]	0.271	Supported
H3b	X3 $\rightarrow$ Z2	0.407	18.399	<0.001	[0.362, 0.450]	0.494	Supported
H3c	X3 $\rightarrow$ Y1	0.086	3.688	<0.001	[0.041, 0.132]	0.018	Supported
H4a	Z1 $\rightarrow$ Y1	-0.219	8.042	<0.001	[-0.271, -0.163]	0.085	Supported
H5a	Z2 $\rightarrow$ Y1	0.453	13.861	<0.001	[0.387, 0.516]	0.279	Supported

Note: β = standardised path coefficient; BC CI = bias-corrected bootstrap confidence interval; f^2 = effect size. X1 = perceived AI convenience; X2 = AI-enabled deception risk; X3 = perceived platform anti-fraud safeguards; Z1 = perceived vulnerability to AI fraud; Z2 = customer trust; Y1 = purchase intention. All direct relationships were significant at $p < 0.001$, and their 95% BC CIs excluded zero

Source: Authors' Work (2025)

Table 2 supports all six mediation hypotheses (all $p < 0.001$; 95% bias-corrected confidence intervals excluded zero). Convenience and safeguards showed positive indirect associations with purchase intention through vulnerability and trust, whereas deception risk showed negative indirect associations. Indirect coefficients were larger through trust ($|\beta| = 0.185\text{--}0.226$) than through vulnerability ($|\beta| = 0.050\text{--}0.133$). Significant direct and indirect relationships operating in the same direction indicate complementary mediation (Zhao et al., 2010), consistent with the proposed parallel mediation model.

Table 3 summarises the combined direct and indirect associations with purchase intention. Deception risk had the largest absolute total coefficient ($\beta = -0.614$), followed by convenience ($\beta = 0.361$) and safeguards ($\beta = 0.346$). Total indirect coefficients were -0.347 , 0.276 , and 0.260 , respectively, exceeding the corresponding direct coefficients in absolute magnitude. These aggregate estimates complement the path-specific results; individual mediation hypotheses were evaluated using the specific indirect effects in Table 2.

Table 2.

Specific indirect effects and mediation hypothesis testing

Hypothesis	Indirect Path	β	t-value	P-value	95% BC CI	Decision
H4b	X2 $\rightarrow$ Z1 $\rightarrow$ Y1	-0.133	7.809	<0.001	[-0.166, -0.099]	Supported
H4c	X3 $\rightarrow$ Z1 $\rightarrow$ Y1	0.075	7.010	<0.001	[0.055, 0.097]	Supported
H4d	X1 $\rightarrow$ Z1 $\rightarrow$ Y1	0.050	6.057	<0.001	[0.035, 0.067]	Supported
H5b	X1 $\rightarrow$ Z2 $\rightarrow$ Y1	0.226	11.704	<0.001	[0.190, 0.267]	Supported
H5c	X2 $\rightarrow$ Z2 $\rightarrow$ Y1	-0.213	11.961	<0.001	[-0.249, -0.179]	Supported
H5d	X3 $\rightarrow$ Z2 $\rightarrow$ Y1	0.185	10.758	<0.001	[0.152, 0.220]	Supported

Note: β = standardised specific indirect coefficient; BC CI = bias-corrected bootstrap confidence interval. X1 = AI convenience; X2 = AI-enabled deception risk; X3 = platform anti-fraud safeguards; Z1 = perceived vulnerability to AI fraud; Z2 = customer trust; Y1 = purchase intention. Indirect effects represent mediation in the parallel model; all were significant ($p < 0.001$), with 95% BC CIs excluding zero

Source: Authors' Work (2025)

Table 3.

Direct, total indirect, and total effects on purchase intention

Predictor	Direct effect	Total indirect effect	Total effect
Perceived AI convenience (X1)	0.086	0.276	0.361
AI-enabled deception risk (X2)	-0.267	-0.347	-0.614
Perceived platform anti-fraud safeguards (X3)	0.086	0.260	0.346

Note: Coefficients are standardised. Total indirect effects sum the specific indirect effects through perceived vulnerability to AI fraud and customer trust; total effects sum direct and total indirect effects. Minor discrepancies in summed coefficients reflect rounding. Aggregate estimates do not determine support for individual mediation hypotheses

Source: Authors' Work (2025)

Discussion

AI convenience, vulnerability, trust, and purchase intention

Perceived AI convenience was associated with lower perceived vulnerability to AI fraud and stronger customer trust. Efficient and predictable shopping interactions may give consumers greater perceived control over product search and evaluation, making the platform appear more manageable and reliable. This interpretation aligns with research linking AI-enabled experiences to reduced effort and greater confidence in digital service providers (Ameen et al., 2021; Chakraborty et al., 2024). Convenience may therefore serve as a cue of platform competence, although perceived ease does not establish that consumers face less objective fraud risk. The relationship concerns how consumers evaluate their exposure within an apparently efficient shopping environment.

The direct relationship between convenience and purchase intention was positive but small, indicating limited practical magnitude despite statistical significance. Previous studies similarly associate AI-related features with purchasing intentions alongside satisfaction, shopping experience, trust, and perceived risk (Arachchi & Samarasinghe, 2025; Santy et al., 2024). Here, the larger indirect coefficient through trust suggests that convenience is particularly relevant when accompanied by confidence in the platform. This pattern qualifies an efficiency-centred explanation of AI adoption: reducing shopping effort alone provides an incomplete account of consumers' willingness to purchase.

AI-enabled deception risk, vulnerability, trust, and purchase intention

AI-enabled deception risk was associated with greater vulnerability and weaker trust. Convincing synthetic reviews, images, and endorsements can complicate authenticity judgments, making consumers feel exposed even when they are familiar with online shopping. Research on AI deception and cyber fraud similarly identifies the capacity of generated content to distort judgments and intensify threat evaluations (Park et al., 2024; Schmitt & Flechais, 2024; Hassan et al., 2024). In this context, doubts about commercial information may extend to the platform's capacity to oversee that information. This offers a plausible interpretation of the negative association with trust, without implying that respondents had experienced verified fraud or that platforms deliberately enabled deception.

Deception risk was also negatively associated with purchase intention and had the largest absolute total coefficient among the three exogenous constructs. This is consistent with research connecting perceived risk to lower purchasing intentions under information asymmetry and uncertainty (Jibril et al., 2020; Sun et al., 2023; Wang et al., 2022). AI adds a specific authenticity problem: persuasive content may appear credible while its origin and accuracy remain difficult to assess. The results suggest that this concern is relevant both directly and through consumers' vulnerability and trust evaluations. The larger total coefficient is descriptive, however, and does not establish a statistically tested difference between predictors.

Platform safeguards, vulnerability, trust, and purchase intention

Perceived platform anti-fraud safeguards were associated with lower vulnerability and stronger trust. Visible verification, warnings, monitoring, and reporting mechanisms may reassure consumers that protection extends beyond their own ability to recognise deception. Related research links security measures and protective responses to digital fraud prevention and threat evaluations (Pitchan et al., 2025; Hassan et al., 2024; Shang et al., 2022). Consumers may also interpret visible safeguards as evidence of platform responsibility and competence (Handoyo, 2024). From an institutional assurance perspective, these

perceptions help explain how platform protection can relate simultaneously to personal exposure and confidence in the transaction environment. The present measures capture perceived safeguards, however, rather than their technical effectiveness.

The positive direct relationship between safeguards and purchase intention was small, while the indirect relationships through vulnerability and trust were more pronounced. This pattern accords with research linking security perceptions to behavioural intentions through trust and perceived risk (Handoyo, 2024). Protective mechanisms may be more relevant to purchasing decisions when consumers recognise them as credible reassurance. Nevertheless, the model did not test whether safeguards weaken the relationship between deception risk and purchase intention; their role should therefore be interpreted as an associated protective perception rather than a demonstrated buffering effect.

Vulnerability and trust as parallel mediators

Vulnerability and trust showed opposing associations with purchase intention. Feeling personally exposed to AI-enabled fraud was associated with lower purchasing intention, whereas confidence in the platform was associated with greater willingness to purchase. These relationships align with evidence on vulnerability, fraud risk, and trust in uncertain digital transactions (Jibril et al., 2020; Handoyo, 2024; Nguyen et al., 2025; Ma et al., 2025). Their distinction matters because personal exposure and platform confidence address different judgments: consumers can acknowledge the possibility of deception while still believing that a platform is competent and responsible. Empirically, however, the proximity of the trust–purchase intention HTMT value to the adopted threshold warrants caution when interpreting their separation.

The specific indirect relationships supported the proposed parallel mediation model. Convenience and safeguards showed positive indirect associations with purchase intention via lower vulnerability and greater trust, whereas deception risk showed negative indirect associations via both mediators. Significant direct and indirect relationships in the same direction were consistent with complementary mediation. Prior research likewise treats risk-related evaluations and trust as relevant mechanisms in digital transaction decisions (Jibril et al., 2020; Handoyo, 2024). Indirect coefficients were larger through trust, although their differences were not formally tested. Moreover, the cross-sectional analysis supports the specified parallel relationships without establishing temporal mediation or excluding alternative sequential models.

Theoretical implications

The study connects AI convenience, deception risk, and perceived platform safeguards within a common framework of consumer decision-making. Its theoretical value lies in distinguishing the functional appeal of AI from concerns

about the authenticity of AI-enabled commercial information, while incorporating institutional protection into the same explanation. Within Protection Motivation Theory, the vulnerability pathway concerns consumers' subjective exposure to threats; the trust pathway draws on institution-based trust and structural assurance. This integration offers a focused application of these perspectives rather than a comprehensive test of all threat and coping appraisal dimensions.

Distinguishing vulnerability from trust also clarifies why favourable purchasing intentions may coexist with awareness of fraud threats. Consumers' assessments of personal exposure need not mirror their confidence in platform competence and integrity. The complementary mediation pattern is consistent with both evaluations contributing additional explanatory pathways alongside the direct relationships. This contribution remains bounded to the measured perceptions of Indonesian users engaged with social and AI-enabled commerce features, with causal ordering and broader applicability requiring further examination.

Managerial and policy implications

Platform managers should develop convenience and protection together. Personalised recommendations and simplified purchasing processes can improve usability, while visible verification, understandable fraud warnings, and accessible reporting channels can address consumers' concerns about authenticity and platform accountability. Given the limited direct effect sizes of convenience and safeguards on purchase intention, implementation should consider whether users understand and trust these features. The findings motivate attention to such design choices, although the effectiveness of individual interventions requires separate evaluation.

Brands and influencers can reduce ambiguity by clearly identifying commercial endorsements and explaining material uses of AI-generated content. Platforms can support these practices through authenticity indicators and transparent complaint and redress procedures. For regulators and industry bodies, the findings underscore the importance of disclosure guidance, consumer protection standards, and education on synthetic reviews and endorsements. In Indonesia, these measures could be evaluated across platforms and consumer groups to determine whether they improve authenticity judgments, confidence in redress, and informed purchasing decisions.

Conclusion, limitations, and future research

This study examined how perceived AI convenience, AI-enabled deception risk, and platform anti-fraud safeguards relate to purchase intention through perceived vulnerability and customer trust among Indonesian social commerce users. Convenience and safeguards were associated with lower vulnerability and stronger trust, whereas deception risk showed the opposite pattern and was

negatively associated with purchase intention. The findings support the proposed parallel mediating roles of vulnerability and trust, integrating AI's functional benefits, deceptive potential, and perceived platform protection within a unified framework.

The cross-sectional design, non-probability sampling, and Indonesian context limit causal inference and generalisability. Potential common-method influence remains unresolved, as full-collinearity VIF values for trust and purchase intention exceeded 3.3 despite remaining below 5.0. The instrument also lacked separately documented expert content validation and formal cognitive pretesting. Future research should strengthen measurement through expert assessment, cognitive interviews, and independent samples; use longitudinal or experimental designs to examine temporal ordering and alternative mediation models; and broaden sampling across populations and platforms. AI literacy, digital resilience, regulatory awareness, and cultural differences warrant examination as potential boundary conditions.

Author contributions

Valentino Aris: Conceptualisation, Investigation, Analysis, Writing – Original Draft. **Idayanti Nursyamsi:** Research Design, Methodology, Supervision. **Arini Lestari Aris:** Data Collection, Analysis, Editing and Formatting. **Muhammad Ashdaq:** Data Analysis, Editing and Formatting.

Declaration of interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

- Almaiah, M. A., Al-Otaibi, S., Shishakly, R., Hassan, L., Lutfi, A., Alrawad, M., Qatawneh, M., & Alghanam, O. A. (2023). Investigating the role of perceived risk, perceived security and perceived trust on smart m-banking application using SEM. *Sustainability*, 15(13), 1–17. <https://doi.org/10.3390/su15139908>.
- Ameen, N., Tarhini, A., Reppel, A., & Anand, A. (2021). Customer experiences in the age of artificial intelligence. *Computers in Human Behavior*, 114, 1–14. <https://doi.org/10.1016/j.chb.2020.106548>.
- Amos, C., & Zhang, L. (2024). Consumer reactions to perceived undisclosed ChatGPT usage in an online review context. *Telematics and Informatics*, 93, 1–15. <https://doi.org/10.1016/j.tele.2024.102163>.
- Arachchi, H. A. D. M., & Samarasinghe, G. D. (2025). Perceived attributes of artificial intelligence (AI) toward consumers' AI attitudes and purchase intention in an AI-powered retail shopping space. *European Journal of Management Studies*, 30(3-4), 243–267. <https://doi.org/10.1108/EJMS-05-2024-0047>.
- Bank Indonesia. (2025). Laporan Perekonomian Indonesia 2024. Bank Indonesia.

- Bekkers, L., van 't Hoff-de Goede, S., Misana-ter Huurne, E., van Houten, Y., Spithoven, R., & Leukfeldt, E. R. (2023). Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model. *Computers & Security*, 127, 1–12. <https://doi.org/10.1016/j.cose.2023.103099>.
- Berry, L. L., Seiders, K., & Grewal, D. (2002). Understanding service convenience. *Journal of Marketing*, 66(3), 1–17. <https://doi.org/10.1509/jmkg.66.3.1.18505>.
- Chakraborty, D., Kar, A. K., Patre, S., & Gupta, S. (2024). Enhancing trust in online grocery shopping through generative AI chatbots. *Journal of Business Research*, 180, 1–18. <https://doi.org/10.1016/j.jbusres.2024.114737>.
- Chung, A., & Yu, Y. (2021). Consumer trust in the digital economy: The case for online dispute resolution (UNCTAD Research Paper No. 72). *United Nations Conference on Trade and Development*.
- Debb, S. M., & McClellan, M. K. (2021). Perceived vulnerability as a determinant of increased risk for cybersecurity risk behavior. *Cyberpsychology, Behavior, and Social Networking*, 24(9), 605–611. <https://doi.org/10.1089/cyber.2021.0043>.
- Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention, and behavior: An introduction to theory and research. Addison-Wesley.
- Gefen, D. (2000). *E-commerce: The role of familiarity and trust*. *Omega*, 28(6), 725–737. [https://doi.org/10.1016/S0305-0483\(00\)00021-9](https://doi.org/10.1016/S0305-0483(00)00021-9).
- Gupta, P., & Hakhu, R. (2021). Impact of perceived security and perceived trust on intention to use digital payments: A study on Indian customers. *Webology*, 18(6), 169–181.
- Hair, J. F., Jr., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). A primer on partial least squares structural equation modeling (PLS-SEM) (2nd ed.). SAGE Publications.
- Hajli, N. (2015). Social commerce constructs and consumer's intention to buy. *International Journal of Information Management*, 35(2), 183–191. <https://doi.org/10.1016/j.ijinfomgt.2014.12.005>.
- Hajli, N., Sims, J., Zadeh, A. H., & Richard, M.-O. (2017). A social commerce investigation of the role of trust in a social networking site on purchase intentions. *Journal of Business Research*, 71, 133–141. <https://doi.org/10.1016/j.jbusres.2016.10.004>.
- Handoyo, S. (2024). Purchasing in the digital age: A meta-analytical perspective on trust, risk, security, and e-WOM in e-commerce. *Heliyon*, 10(8), 1–23. <https://doi.org/10.1016/j.heliyon.2024.e29714>.
- Hassan, S., Ahmad, R., Katuk, N., Ghazali, N. N., Aripin, J. A., & Ali, F. (2024). Staying one step ahead: Exploring Protection Motivation Theory to combat cyber-fraud among e-services users. *Procedia Computer Science*, 234, 1364–1371. <https://doi.org/10.1016/j.procs.2024.04.011>.
- Iwara, I. O. (2025). Law enforcement impersonation bank-related scams in South Africa: Perceived vulnerability and mitigative strategies. *Risks*, 13(8), 1–16. <https://doi.org/10.3390/risks13080156>.

- Jiang, L. (Alice), Yang, Z., & Jun, M. (2013). Measuring consumer perceptions of online shopping convenience. *Journal of Service Management*, 24(2), 191–214. <https://doi.org/10.1108/09564231311323962>.
- Jibril, A. B., Kwarteng, M. A., Botchway, R. K., Bode, J., & Chovancova, M. (2020). The impact of online identity theft on customers' willingness to engage in e-banking transaction in Ghana: A technology threat avoidance theory. *Cogent Business & Management*, 7(1), 1–22. <https://doi.org/10.1080/23311975.2020.1832825>.
- Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, 44(2), 544–564. <https://doi.org/10.1016/j.dss.2007.07.001>.
- Lo Presti, L., & Maggiore, G. (2023). Vulnerability on collaborative networks and customer engagement: Defending the online customer experience from fake reviews. *Quality & Quantity*, 57(3), 449–463. <https://doi.org/10.1007/s11135-021-01249-w>.
- Lopes, J. M., Silva, L. F., & Massano-Cardoso, I. (2024). AI meets the shopper: Psychosocial factors in ease of use and their effect on e-commerce purchase intention. *Behavioral Sciences*, 14(7), 1–22. <https://doi.org/10.3390/bs14070616>.
- Ma, D., Dong, J., & Lee, C. C. (2025). Influence of perceived risk on consumers' intention and behavior in cross-border e-commerce transactions: A case study of the Tmall Global platform. *International Journal of Information Management*, 81, 1–29. <https://doi.org/10.1016/j.ijinfomgt.2024.102854>.
- Marwi, H. C., & Oskar, I. (2023). Analysis of increasing types of online fraud and level of public awareness in Indonesia. *Journal of Embedded System Security and Intelligence System*, 4(2), 69–83. <https://doi.org/10.59562/jessi.v4i2.722>.
- McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, 13(3), 334–359. <https://doi.org/10.1287/isre.13.3.334.81>.
- Meng, W., Harvey, J., Goulding, J., Carter, C. J., Lukinova, E., Smith, A., Frobisher, P., Forrest, M., & Nica-Avram, G. (2025). Large language models as “hidden persuaders”: Fake product reviews are indistinguishable to humans and machines. *arXiv*. <https://doi.org/10.48550/arXiv.2506.13313>.
- Mulyadi, M., Nurdin, A. A., Anjani, A. A., Alamsyah, F. D., Sifana, F., Yudistio, M. A., Maulana, M. K., & Rabbani, R. A. A. (2024). Analisis penipuan online melalui media sosial dalam perspektif kriminologi. *Media Hukum Indonesia*, 2(2), 74–82. <https://doi.org/10.5281/zenodo.11183088>.
- Nguyen, T. T., Nguyen, H. T., Nguyen, A. V., Tran, P. T., Mai, H. N., & Pham, T. V. A. (2025). Consumers' vulnerability and e-commerce purchase behavior: A serial mediation model. *Telematics and Informatics Reports*, 18, 1–11. <https://doi.org/10.1016/j.teler.2025.100215>.
- Nurdianasari, R., Maharani, S., & Damarani, Z. N. (2025). The role of online convenience in enhancing customer satisfaction and behavioral intention.

- International Research Journal of Economics and Management Studies*, 4(5), 267–276. <https://doi.org/10.56472/25835238/IRJEMS-V4I5P135>.
- Park, P. S., Goldstein, S., O’Gara, A., Chen, M., & Hendrycks, D. (2024). AI deception: A survey of examples, risks, and potential solutions. *Patterns*, 5(5), 1–16. <https://doi.org/10.1016/j.patter.2024.100988>.
- Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the Technology Acceptance Model. *International Journal of Electronic Commerce*, 7(3), 101–134. <https://doi.org/10.1080/10864415.2003.11044275>.
- Pitchan, M. A., Salman, A., & Arib, N. M. (2025). A systematic literature review on online scams: Insights into digital literacy, technological innovations, and victimology. *Jurnal Komunikasi: Malaysian Journal of Communication*, 41(1), 107–124. <https://doi.org/10.17576/JKMJC-2025-4101-07>.
- Qu, J., Lin, K., Wu, Y., & Sun, I. Y. (2024). Fear and perceived risk of cyber fraud victimization among Chinese university students. *Crime, Law and Social Change*, 82(3), 543–562. <https://doi.org/10.1007/s10611-024-10155-9>.
- Regula. (2024). Deepfake trends 2024. <https://regulaforensics.com/resources/deepfake-trends-2024-report/>.
- Rejikumar, G., Dinesh, K. G. S., Asokan-Ajitha, A., & Jose, A. (2021). Privacy breach perceptions and litigation intentions: Evidence from e-commerce customers. *IIMB Management Review*, 33(4), 322–336. <https://doi.org/10.1016/j.iimb.2021.11.001>.
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93–114. <https://doi.org/10.1080/00223980.1975.9915803>.
- Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153–176). Guilford Press.
- Salminen, J., Kandpal, C., Kamel, A. M., Jung, S., & Jansen, B. J. (2022). Creating and detecting fake reviews of online products. *Journal of Retailing and Consumer Services*, 64, 1–15. <https://doi.org/10.1016/j.jretconser.2021.102771>.
- Santy, R. D., Hamdani, M. G. Q., & Rahma, S. J. A. (2024). Enhancing online purchase intention through artificial intelligence: Transformation to digital customer experience. In *Proceedings of the International Conference on Business, Economics, Social Sciences, and Humanities: Economics, Business and Management Track (ICOBEST-EBM 2024)* (pp. 120–135). Atlantis Press. https://doi.org/10.2991/978-94-6463-465-5_11.
- Saxena, C., & Thakur, P. (2024). Mediating role of trust and privacy concerns between web assurance mechanism and purchase intention of online products. *Telematics and Informatics Reports*, 16, 1–10. <https://doi.org/10.1016/j.teler.2024.100177>.

- Schmitt, M., & Flechais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review*, 57(12), 1–24. <https://doi.org/10.1007/s10462-024-10973-2>.
- Senali, M. G., Iranmanesh, M., Ghobakhloo, M., Foroughi, B., Asadi, S., & Rejeb, A. (2024). Determinants of trust and purchase intention in social commerce: Perceived price fairness and trust disposition as moderators. *Electronic Commerce Research and Applications*, 64, 1–13. <https://doi.org/10.1016/j.elerap.2024.101370>.
- Shang, Y., Wu, Z., Du, X., Jiang, Y., Ma, B., & Chi, M. (2022). The psychology of the internet fraud victimization of older adults: A systematic review. *Frontiers in Psychology*, 13, 1–15. <https://doi.org/10.3389/fpsyg.2022.912242>.
- Sintia, L., Siagian, Y., & Kurniawati, K. (2023). The determinants of purchase intention in social commerce. *Jurnal Manajemen Bisnis*, 14, 214–237. <https://doi.org/10.18196/mb.v14i1.15754>.
- Spears, N., & Singh, S. N. (2004). Measuring attitude toward the brand and purchase intentions. *Journal of Current Issues & Research in Advertising*, 26(2), 53–66. <https://doi.org/10.1080/10641734.2004.10505164>.
- Sun, X., Pelet, J.-É., Dai, S., & Ma, Y. (2023). The effects of trust, perceived risk, innovativeness, and deal proneness on consumers' purchasing behavior in the livestreaming social commerce context. *Sustainability*, 15(23), 1–14. <https://doi.org/10.3390/su152316320>.
- Valencia-Arias, A., Uribe-Bedoya, H., González-Ruiz, J. D., Santos, G. S., Ramírez, E. C., & Rojas, E. M. (2024). Artificial intelligence and recommender systems in e-commerce: Trends and research agenda. *Intelligent Systems with Applications*, 24, 1–15. <https://doi.org/10.1016/j.iswa.2024.200435>.
- Wagner, G., Fota, A., Schramm-Klein, H., & Steinmann, S. (2023). Development of a Motivation-Trust-Vulnerability (MTV) framework for cross-border online shopping: A cross-national application to Chinese and German consumers. *Schmalenbach Journal of Business Research*, 75(3), 389–414. <https://doi.org/10.1007/s41471-023-00170-2>.
- Wang, J., Shahzad, F., Ahmad, Z., Abdullah, M., & Hassan, N. M. (2022). Trust and consumers' purchase intention in a social commerce platform: A meta-analytic approach. *SAGE Open*, 12(2), 1–15. <https://doi.org/10.1177/21582440221091262>.
- Williamson, S. M., & Prybutok, V. (2024). The era of artificial intelligence deception: Unraveling the complexities of false realities and emerging threats of misinformation. *Information*, 15(6), 1–43. <https://doi.org/10.3390/info15060299>.
- Xylogiannopoulos, K. F., Xanthopoulos, P., Karampelas, P., & Bakamitsos, G. A. (2024). ChatGPT paraphrased product reviews can confuse consumers and undermine their trust in genuine reviews. Can you tell the difference? *Information Processing & Management*, 61(6), 1–18. <https://doi.org/10.1016/j.ipm.2024.103842>.
- Yin, J., Qiu, X., & Wang, Y. (2025). The impact of AI-personalized recommendations on clicking intentions: Evidence from Chinese e-

Aris, V., Nursyamsi, I., Aris, A. L., & Ashdaq, M.
The double-edged sword of artificial intelligence in social commerce: how
convenience, AI-enabled deception risk, and anti-fraud safeguards shape
vulnerability, trust, and purchase intention

commerce. *Journal of Theoretical and Applied Electronic Commerce
Research*, 20(1), 1–40. <https://doi.org/10.3390/jtaer20010021>.

Zhao, X., Lynch, J. G., Jr., & Chen, Q. (2010). Reconsidering Baron and Kenny:
Myths and truths about mediation analysis. *Journal of Consumer Research*,
37(2), 197–206. <https://doi.org/10.1086/651257>.

Appendix 1.
Respondent demographics

	Indicators	f	Percentage
Gender	Male	199	28%
	Female	521	72%
Occupation	Student	288	40%
	Private sector employee	252	35%
	Civil servant / state-owned enterprise employee	108	15%
	Entrepreneurs	50	7%
	Other	22	3%
Age	18 – 25 years	456	63%
	26 – 33 years	120	17%
	34 – 40 years	84	12%
	41 – 47 years	60	8%
Education	High school	329	46%
	Bachelor	230	32%
	Master	95	13%
	Doctorate	66	9%

Source: Authors' Work (2025)

Appendix 2.
Measurement items

Construct	Items	Original item wording or conceptual basis	Exact source	Adaptation type
Perceived AI convenience (X1)	AI features help me find products faster.	Original item: "I am able to find desired products quickly."	Jiang et al. (2013), Appendix 2, Search Convenience.	Contextual adaptation
	AI features make searching and filtering products easier.	Search convenience involving ease of navigation, product classification, and locating products.	Jiang et al. (2013), Appendix 2, Search Convenience; Lopes et al. (2024), AI-enabled ease of use in e-retail.	Contextual reformulation
	AI recommendations reduce my effort to find suitable products.	Search and evaluation convenience, particularly lower effort in locating and evaluating products.	Jiang et al. (2013), Appendix 2, Search and Evaluation Convenience; Lopes et al. (2024).	Contextual reformulation

Aris, V., Nursyamsi, I., Aris, A. L., & Ashdaq, M.

The double-edged sword of artificial intelligence in social commerce: how convenience, AI-enabled deception risk, and anti-fraud safeguards shape vulnerability, trust, and purchase intention

Construct	Items	Original item wording or conceptual basis	Exact source	Adaptation type
AI-enabled deception risk (X2)	The AI system simplifies the purchase process.	Original item: "I am able to complete my purchases without difficulty."	Jiang et al. (2013), Appendix 2, Transaction Convenience.	Contextual adaptation
	AI features help me make purchase decisions faster.	Overall online-shopping convenience concerns reductions in consumers' time and effort; recent AI retail research also conceptualizes AI-enabled ease of use as facilitating online purchasing.	Jiang et al. (2013), overall convenience framework; Lopes et al. (2024), AI-enabled ease of use.	Contextually developed
	Overall, AI makes my shopping experience more convenient.	Global appraisal of convenience across AI-enabled shopping activities. No directly equivalent original item is claimed.	Jiang et al. (2013), overall online-shopping convenience framework; Lopes et al. (2024).	Contextually developed
	I worry AI can create misleading reviews or product content.	AI deception can create false beliefs; consumers perceive ChatGPT-generated reviews as less trustworthy and authentic than human-generated reviews.	Park et al. (2024), AI deception; Amos & Zhang (2024), AI-generated online reviews.	Contextually developed
	I see a risk that AI-made images or videos may misrepresent the product.	Generative AI enables realistic synthetic text, images, audio, and video that can facilitate digital deception.	Schmitt & Flechais (2024), Realistic Content Creation; Park et al. (2024).	Contextually developed
	I feel AI-assisted information can be manipulated to influence my decisions.	AI-enabled deception can involve manipulation and persuasive, personalized deceptive content.	Park et al. (2024); Schmitt & Flechais (2024), Generative AI Social Engineering Framework.	Contextually developed
	I think the chance of being deceived by AI content here is quite high.	AI deception presents fraud and manipulation risks, while generative AI increases the realism and scalability of deceptive content.	Park et al. (2024); Schmitt & Flechais (2024).	Contextually developed
	It's hard to tell if reviews or information are human-written or AI-generated.	Recent evidence shows that AI-paraphrased or AI-generated fake reviews can be difficult to distinguish from authentic reviews.	Xylogiannopoulos et al. (2024); Meng et al. (2025).	Contextually developed
	I believe fraudsters can use AI on this platform to deceive users like me.	Fraud is identified as a risk arising from AI deception, while generative AI can strengthen phishing and social-engineering attacks.	Park et al. (2024); Schmitt & Flechais (2024).	Contextually developed

Aris, V., Nursyamsi, I., Aris, A. L., & Ashdaq, M.

The double-edged sword of artificial intelligence in social commerce: how convenience, AI-enabled deception risk, and anti-fraud safeguards shape vulnerability, trust, and purchase intention

Construct	Items	Original item wording or conceptual basis	Exact source	Adaptation type
Perceived platform anti-fraud safeguards (X3)	I believe this platform strongly verifies suspicious sellers, ads, and accounts.	Structural assurance concerns institutional and technological structures that protect consumers; newer web-assurance research emphasizes visible protection mechanisms.	McKnight et al. (2002), Appendix, Structural Assurance; Saxena & Thakur (2024), Web Assurance Mechanism.	Contextually developed
	This platform clearly warns users about potential online fraud.	Structural assurance and web assurance communicate that protective structures are in place to reduce online transactional risk.	McKnight et al. (2002), Structural Assurance; Saxena & Thakur (2024).	Contextually developed
	This platform offers an easy way to report fraud.	Consumer reporting and dispute-resolution mechanisms function as institutional mechanisms for consumer protection and trust.	Chung & Yu (2021), UNCTAD Research Paper No. 72; Saxena & Thakur (2024).	Contextually developed
	I believe this platform responds quickly to reported fraud cases.	Effective consumer dispute-resolution mechanisms can strengthen trust and provide institutional protection after transaction problems occur.	Chung & Yu (2021), UNCTAD Research Paper No. 72.	Contextually developed
	Overall, I feel this platform has adequate protection against AI-based fraud.	Structural assurance reflects confidence that legal and technological structures protect users; web assurance mechanisms similarly provide credibility and protection.	McKnight et al. (2002), Appendix, Structural Assurance; Saxena & Thakur (2024).	Contextual reformulation
Perceived vulnerability to AI fraud (Z1)	I feel personally vulnerable to AI-based fraud on social commerce.	Perceived cybersecurity vulnerability concerns individuals' perception of their own vulnerability to cyber victimization.	Debb & McClellan (2021), Perceived Vulnerability domain.	Contextually developed
	Even if I'm careful, I still feel a high chance of being deceived by AI fraud.	Personal vulnerability concerns perceived exposure to victimization; cyber-fraud research separately recognizes perceived vulnerability in threat appraisal.	Debb & McClellan (2021); Hassan et al. (2024).	Contextual reformulation
	Compared to other users, I feel more vulnerable to AI-based online fraud.	Subjective consumer vulnerability reflects perceived personal exposure relative to one's ability to navigate online risks.	Debb & McClellan (2021); Wagner et al. (2023), consumer vulnerability in online shopping.	Contextually developed

Aris, V., Nursyamsi, I., Aris, A. L., & Ashdaq, M.

The double-edged sword of artificial intelligence in social commerce: how convenience, AI-enabled deception risk, and anti-fraud safeguards shape vulnerability, trust, and purchase intention

Construct	Items	Original item wording or conceptual basis	Exact source	Adaptation type
Customer trust (Z2)	If I'm not very vigilant, my chances of loss from AI fraud are quite high.	Vulnerability concerns perceived exposure to cyber victimization; cyber-fraud research also emphasizes the challenge of detecting increasingly sophisticated fraud.	Debb & McClellan (2021); Hassan et al. (2024).	Contextual reformulation
	I believe this platform is honest in presenting information.	Original integrity item: "I would characterize LegalAdvice.com as honest."	McKnight et al. (2002), Appendix, Trusting Beliefs: Integrity, Item 2.	Contextual adaptation
	I'm confident this platform prioritizes its users' interests.	Original benevolence item: "I believe that LegalAdvice.com would act in my best interest."	McKnight et al. (2002), Appendix, Trusting Beliefs: Benevolence, Item 1.	Contextual adaptation
	This platform is competent in managing transactions and its AI technology.	Trusting-belief competence items assess whether the vendor is competent, effective, capable, and knowledgeable.	McKnight et al. (2002), Appendix, Trusting Beliefs: Competence, Items 1–4.	Contextual reformulation
Purchase intention (Y1)	I generally trust this platform not to misuse my data when I use it.	Online trust reduces concerns arising from informational vulnerability and uncertainty in e-commerce transactions.	McKnight et al. (2002); Pavlou (2003).	Contextually developed
	Overall, I have a high level of trust in this social commerce platform.	Original global trust item: "I trust Amazon.com."	Gefen (2000), Appendix A, Trust, Tr2.	Contextual adaptation
	I intend to keep buying products through AI-enabled social commerce.	Continued online shopping and intention to transact are established favorable future behavioral intentions.	Jiang et al. (2013), Appendix 2, Behavioral Intentions; Pavlou (2003), Intention to Transact.	Contextual reformulation
	I am very likely to make another purchase through this platform soon.	Original item: "I am very likely to buy books from Amazon.com."	Gefen (2000), Appendix A, Buy3.	Contextual adaptation
	When I want to shop, I will consider AI-based platform as a primary option.	Spears and Singh conceptualize purchase intention as personal action tendencies toward purchasing and operationalize it with intention, likelihood, and purchase-interest judgments.	Spears & Singh (2004), Appendix 1, Purchase Intentions; Pavlou (2003), Intention to Transact.	Contextual reformulation

Aris, V., Nursyamsi, I., Aris, A. L., & Ashdaq, M.

The double-edged sword of artificial intelligence in social commerce: how convenience, AI-enabled deception risk, and anti-fraud safeguards shape vulnerability, trust, and purchase intention

Construct	Items	Original item wording or conceptual basis	Exact source	Adaptation type
	If I find suitable products, I'm willing to buy via AI-based social commerce.	Purchase intention encompasses willingness, likelihood, and deliberate intention to purchase; intention to transact represents willingness to engage in an online transaction.	Spears & Singh (2004) , Purchase Intentions; Pavlou (2003) , Intention to Transact.	Contextual reformulation
	Willing to increase my purchase frequency on AI-based social commerce.	Jiang et al.'s behavioral-intention scale includes greater future use of the retailer for online purchasing.	Jiang et al. (2013) , Appendix 2, Behavioral Intentions, Item 3.	Contextual reformulation

Note. Five indicators (X3_6, Z1_3, Z1_6, Z2_4, and Y1_4) were excluded following item-level conceptual reassessment. The exclusions were based on construct-domain correspondence rather than statistical performance alone. The original item codes of the retained indicators were preserved to maintain traceability with the questionnaire and dataset

Source: Authors' Work (2025)

Appendix 2.

Measurement model evaluation

Variable	Items	Outer Loading	Cronbach's Alpha	Rho_A	Rho_C	AVE
X1	Perceived AI convenience		0.916	0.918	0.935	0.704
	X1_1	0.856				
	X1_2	0.831				
	X1_3	0.851				
	X1_4	0.833				
	X1_5	0.833				
	X1_6	0.830				
X2	AI-enabled deception risk		0.918	0.919	0.936	0.708
	X2_1	0.863				
	X2_2	0.840				
	X2_3	0.847				
	X2_4	0.831				
	X2_5	0.824				
	X2_6	0.845				
X3	Perceived platform anti-fraud safeguards		0.901	0.902	0.926	0.716
	X3_1	0.839				
	X3_2	0.841				
	X3_3	0.829				
	X3_4	0.866				
	X3_5	0.856				
Z1	Perceived vulnerability to AI fraud		0.881	0.881	0.918	0.737
	Z1_1	0.856				
	Z1_2	0.850				
	Z1_4	0.865				
	Z1_5	0.863				
Z2	Customer trust		0.899	0.899	0.925	0.713
	Z2_1	0.838				
	Z2_2	0.842				
	Z2_3	0.850				
	Z2_5	0.857				
	Z2_6	0.834				
Y1	Purchase intention		0.904	0.904	0.929	0.722
	Y1_1	0.856				
	Y1_2	0.845				
	Y1_3	0.854				
	Y1_5	0.852				
	Y1_6	0.843				

Source: Authors' Work (2025)

Appendix 3.

Fornell-Larcker criterion

	X2	Z2	X1	X3	Z1	Y1
X2	0.842					
Z2	-0.503	0.844				
X1	-0.031	0.512	0.839			
X3	-0.041	0.425	-0.003	0.846		
Z1	0.628	-0.621	-0.244	-0.368	0.858	
Y1	-0.639	0.804	0.379	0.370	-0.721	0.850

Source: Authors' Work (2025)

Appendix 4.

Heterotrait-Monotrait ratio (HTMT)

	X2	Z2	X1	X3	Z1	Y1
X2						
Z2	0.552					
X1	0.038	0.563				
X3	0.047	0.472	0.040			
Z1	0.698	0.696	0.270	0.412		
Y1	0.701	0.892	0.416	0.409	0.808	

Source: Authors' Work (2025)

Appendix 5.

Excluded indicators following conceptual reassessment

Indicator	Variable	Initial item wording	Reason for exclusion	Final status
X3_6	Perceived platform anti-fraud safeguards	I feel safe transacting here because of its clear anti-fraud measures.	The item primarily reflects perceived transactional safety as an outcome of protection rather than consumers' perceptions of the platform's anti-fraud safeguard mechanisms.	Excluded
Z1_3	Perceived vulnerability to AI fraud	I'm not very confident I can always recognize AI-based fraud attempts.	The item primarily reflects confidence in recognizing or detecting AI-enabled fraud, which is conceptually closer to self-efficacy than to perceived vulnerability.	Excluded
Z1_6	Perceived vulnerability to AI fraud	I would suffer significant losses if I became a victim of AI-based fraud on this platform.	The item primarily captures the perceived severity of potential consequences rather than consumers' perceived susceptibility or personal vulnerability to AI-enabled fraud.	Excluded
Z2_4	Customer trust	I feel I can rely on this platform when purchasing through AI-based features.	The item reflects willingness to depend on the platform, which is conceptually closer to trusting intention than to the trusting beliefs represented by the retained Customer Trust indicators.	Excluded
Y1_4	Purchase intention	I will recommend others to make purchases through this platform.	The item primarily represents recommendation or word-of-mouth intention rather than the respondent's own intention to purchase.	Excluded

Source: Authors' Work (2025)

Appendix 6.

Full-collinearity VIF assessment of potential common method bias

Construct	R ² from Full-Collinearity regression	Full-Collinearity VIF
Perceived AI convenience (X1)	0.452	1.824
AI-enabled deception risk (X2)	0.619	2.623
Perceived platform anti-fraud safeguards (X3)	0.415	1.710
Perceived vulnerability to AI fraud (Z1)	0.606	2.536
Customer trust (Z2)	0.743	3.894
Purchase intention (Y1)	0.758	4.134

Source: Authors' Work (2025)