

Analysis of Privacy Protection Mechanism and Information Security Policy as Antecedents of User Trust in E-Commerce Platforms in Indonesia

Agus Purwanto¹, Joko Santoso², Affan Irfan Fauziawan³, I Wayan Karang Utama⁴, Anggun Nugroho⁵

¹⁻⁵ Institut Teknologi dan Bisnis STIKOM Bali

Article Info

Article history:

Received Aug, 2026

Revised Aug, 2026

Accepted Aug, 2026

Keywords:

E-Commerce

Information Security Policies

Privacy Protection Mechanisms

User Trust

Indonesia

ABSTRACT

The rapid growth of e-commerce in Indonesia has increased the importance of personal data protection and information security in building consumer confidence. This study analyzes the effects of Privacy Protection Mechanisms and Information Security Policies on User Trust in e-commerce platforms in Indonesia. A quantitative research approach was employed using a cross-sectional survey involving 150 respondents who had experience using e-commerce platforms. Data were collected through a structured questionnaire measured using a five-point Likert scale and analyzed using Partial Least Squares Structural Equation Modeling with SmartPLS 3. The measurement model demonstrated satisfactory reliability and validity. The structural model showed that Privacy Protection Mechanisms had a positive and significant effect on User Trust, while Information Security Policies also had a positive and significant effect on User Trust. The model explained 61.7% of the variance in User Trust, with an R^2 value of 0.617 and a Q^2 value of 0.428, indicating satisfactory explanatory and predictive relevance. Information Security Policies emerged as the strongest predictor of User Trust. These findings confirm that both privacy governance and information security management are essential for strengthening consumer confidence in e-commerce platforms. E-commerce providers should therefore improve privacy transparency, user control, authentication, transaction security, fraud prevention, and incident response mechanisms to support sustainable digital trust.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Name: Agus Purwanto

Institution: Institut Teknologi dan Bisnis STIKOM Bali

Email: agus712@gmail.com

1. INTRODUCTION

The rapid development of digital technology has significantly transformed commercial activities and consumer behavior, particularly through the increasing use of e-commerce platforms. These platforms enable

consumers to search for products, compare alternatives, communicate with sellers, make payments, and complete transactions through integrated digital systems [1]–[3]. In Indonesia, the expansion of e-commerce has been supported by increasing internet penetration, widespread smartphone

adoption, the development of digital payment systems, and changing consumer preferences toward online transactions [3]–[5]. Although this development provides substantial benefits in terms of accessibility, efficiency, convenience, and market reach, it also creates important challenges concerning the protection of consumers' personal information. The increasing dependence on digital platforms means that consumers must disclose various types of personal and transactional data, making privacy protection an increasingly important consideration in maintaining confidence in e-commerce activities [6], [7].

E-commerce transactions require consumers to provide information such as names, telephone numbers, email addresses, delivery addresses, account credentials, payment information, purchasing histories, and browsing activities. This information enables e-commerce providers to authenticate users, process transactions, personalize services, prevent fraud, and maintain customer relationships [8]–[10]. However, extensive collection and processing of personal information may also create privacy concerns when consumers have limited knowledge regarding how their information is collected, stored, processed, shared, and retained. Consumers may become concerned about unauthorized use of their personal data, disclosure to third parties, excessive data collection, or insufficient control over their personal information [11]–[13]. These concerns can increase consumers' perceptions of vulnerability and influence their willingness to provide information and conduct transactions through e-commerce platforms.

Privacy protection mechanisms therefore represent an important component of e-commerce governance. These mechanisms encompass organizational, procedural, and technological measures designed to ensure that consumers' personal information is collected and processed appropriately and responsibly [14], [15]. They may include transparent privacy notices, informed consent procedures, restrictions on unnecessary data collection, consumer control

over personal information, confidentiality safeguards, and clear procedures governing data sharing and retention. In Indonesia, the importance of these mechanisms has become increasingly evident following the enactment of Law Number 27 of 2022 concerning Personal Data Protection, which strengthens the legal framework governing personal data processing. Nevertheless, regulatory compliance alone may not automatically generate consumer confidence because users must also perceive that privacy protection measures are effectively implemented, transparently communicated, and consistently applied by e-commerce platforms.

User trust becomes particularly important in this context because e-commerce transactions are characterized by uncertainty, information asymmetry, and limited physical interaction between consumers and service providers. Consumers are generally unable to directly observe how an e-commerce company manages its databases, processes personal information, shares user data, or implements internal privacy procedures [16], [17]. Consequently, users must rely on their perceptions regarding whether the platform behaves responsibly, maintains integrity, and protects their interests. User trust can therefore be understood as consumers' willingness to rely on an e-commerce platform based on expectations regarding its reliability, integrity, competence, and responsible behavior [1], [18]. Higher levels of trust may encourage consumers to disclose necessary personal information, complete transactions, use digital payment services, repurchase products, and maintain long-term relationships with the platform.

The relationship between privacy protection mechanisms and user trust can be explained through the vulnerability associated with personal information disclosure. Consumers must provide personal information to access various digital services, while their ability to monitor subsequent data-processing activities is relatively limited. Effective privacy protection mechanisms can reduce this vulnerability by increasing transparency, user control, and organizational

accountability [14], [19]. Clear information concerning data collection purposes, consent procedures, data-sharing practices, retention policies, and consumers' privacy rights can strengthen perceptions that the platform handles personal information responsibly. Previous studies on e-commerce have recognized privacy, perceived risk, security, service quality, reputation, and technological reliability as important determinants of consumer trust. However, privacy is frequently incorporated into broader constructs such as perceived risk or perceived security, which may obscure the specific contribution of privacy protection mechanisms to trust formation.

This issue creates an important research gap, particularly in the rapidly developing Indonesian e-commerce environment. The increasing volume of online transactions and personal data processing, accompanied by growing public awareness of data leakage and misuse of personal information, has strengthened consumers' expectations regarding transparency, control, and accountability. However, empirical research that specifically positions privacy protection mechanisms as an independent predictor of user trust remains relatively limited compared with studies focusing on technology acceptance, perceived usefulness, service quality, satisfaction, or purchase intention. Therefore, this study specifically addresses the first research question: Do privacy protection mechanisms have a positive and significant effect on user trust in e-commerce platforms in Indonesia? Accordingly, the study aims to empirically examine the effect of privacy protection mechanisms on user trust. The findings are expected to contribute theoretically to the digital trust and e-commerce literature while providing practical implications for e-commerce providers in developing transparent, accountable, and consumer-oriented privacy practices that can strengthen sustainable user trust.

2. LITERATURE REVIEW

2.1 Theoretical Foundation

The development of trust in e-commerce can be explained through institution-based trust, particularly structural assurance, which emphasizes the role of legal, technological, and organizational safeguards in reducing uncertainty [1], [18]. In digital transactions, consumers disclose personal and financial information without directly observing how platforms manage and protect the data. Privacy protection mechanisms and information security policies therefore function as structural assurances that strengthen perceptions of platform reliability [20], [21]. Privacy protection focuses on the responsible collection, use, storage, and disclosure of personal information, while information security focuses on protecting data and systems from unauthorized access and other threats. Although related, both represent distinct mechanisms that can contribute to user trust in e-commerce platforms.

2.2 E-Commerce Platforms

The development of trust in e-commerce can be explained through institution-based trust, particularly structural assurance, which emphasizes the role of legal, technological, and organizational safeguards in reducing uncertainty. In digital transactions, consumers disclose personal and financial information without directly observing how platforms manage and protect the data [11], [18]. Privacy protection mechanisms and information security policies therefore function as structural assurances that strengthen perceptions of platform reliability. Privacy

protection focuses on the responsible collection, use, storage, and disclosure of personal information, while information security focuses on protecting data and systems from unauthorized access and other threats [22], [23]. Although related, both represent distinct mechanisms that can contribute to user trust in e-commerce platforms.

2.3 Privacy Protection Mechanisms

Privacy protection mechanisms refer to policies, procedures, organizational practices, and technological measures designed to protect personal information and provide users with appropriate control over its processing. In e-commerce, these mechanisms cover the collection, use, storage, disclosure, retention, and deletion of user data [24]–[26]. Key aspects include transparency regarding data practices, user consent and control, data minimization, purpose limitation, and responsible third-party data sharing. In Indonesia, these practices are increasingly reinforced by Law Number 27 of 2022 concerning Personal Data Protection [3], [5]. Effective privacy protection can reduce information asymmetry and perceived vulnerability while signaling organizational responsibility and integrity, thereby strengthening consumer confidence and trust in e-commerce platforms.

2.4 Information Security Policies

Information security refers to the protection of information and information systems by maintaining confidentiality, integrity, and availability. In e-commerce, information security

policies establish organizational requirements, procedures, responsibilities, and controls related to authentication, access management, password protection, payment security, data transmission, fraud prevention, system monitoring, and incident response [27], [28]. Security mechanisms such as multi-factor authentication, encryption, transaction verification, access controls, and fraud detection can reduce the risk of unauthorized access and financial loss. Effective security policies also require continuous monitoring, vulnerability assessment, system updates, and rapid responses to security incidents because cybersecurity threats continue to evolve [15], [29]. From the perspective of user trust, consistent and visible security measures indicate platform competence and reliability, reduce perceived technological risk, and strengthen users' confidence that their accounts, personal information, and transactions are adequately protected.

2.5 User Trust

Trust is a multidimensional concept that reflects an individual's willingness to rely on another party under conditions of uncertainty and vulnerability. In e-commerce, user trust is especially important because consumers transact without direct physical interaction and often provide personal or financial information before receiving the expected benefits [16], [17]. Trust is commonly associated with perceptions of competence, integrity, reliability, and benevolence, which shape users' confidence in a platform's ability

and willingness to act responsibly. A high level of trust can reduce perceived uncertainty and encourage consumers to disclose information, make payments, continue using the platform, repurchase, remain loyal, and provide positive recommendations. Privacy and security are therefore important foundations of trust because they directly relate to consumers' vulnerability concerning data use and unauthorized access [19], [28]. However, trust is broader than perceived privacy or security because it depends on whether protective mechanisms are considered credible, effective, and consistently implemented.

2.6 Privacy Protection Mechanisms and User Trust

Privacy protection mechanisms are expected to positively influence user trust because the disclosure of personal data places consumers in a vulnerable position and requires them to rely on e-commerce platforms to manage their information responsibly. Transparent explanations regarding data collection, processing purposes, data sharing, and user rights can reduce uncertainty and strengthen perceptions of organizational integrity [3], [30]. User control through privacy preferences, informed consent, access to personal information, and available data rights can also reduce dependence on unilateral platform decisions and increase confidence in data governance practices. From the perspective of structural assurance, privacy protection mechanisms represent formal safeguards that

create more predictable and acceptable conditions for digital transactions [8], [31]. Therefore, stronger privacy protection mechanisms are expected to increase user trust in e-commerce platforms, leading to the hypothesis that privacy protection mechanisms have a positive and significant effect on user trust.

H1: Privacy Protection Mechanisms have a positive and significant effect on User Trust in e-commerce platforms in Indonesia.

2.7 Information Security Policies and User Trust

Information security policies are expected to positively influence user trust because consumers face technological and financial risks such as unauthorized account access, payment fraud, identity misuse, and data breaches when using e-commerce platforms. Security measures, including authentication, secure payment procedures, transaction verification, access controls, fraud prevention, and incident response, can signal platform competence and reliability [8], [32]. Clear communication regarding these security practices can also reduce information asymmetry by providing users with observable evidence of otherwise invisible protection processes. From the perspective of structural assurance, information security policies establish formal safeguards that reduce uncertainty and strengthen perceptions of safe digital interaction [31], [33]. Therefore, stronger information security policies are expected to increase user trust in e-commerce

platforms, leading to the hypothesis that information security policies have a positive and significant effect on user trust.

H2: Information Security Policies have a positive and significant effect on User Trust in e-commerce platforms in Indonesia.

3. METHODS

3.1 Research Design

This study employed a quantitative approach with a cross-sectional survey design to examine the influence of Privacy Protection Mechanisms (PPM) and Information Security Policies (ISP) on User Trust (UT) in e-commerce platforms in Indonesia. The quantitative approach was used to measure relationships among latent constructs based on respondents' numerical perceptions, while the cross-sectional design enabled data collection at a single point in time. PPM and ISP were treated as exogenous variables, whereas UT served as the endogenous variable. The relationships among these constructs were analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM), which enables simultaneous evaluation of the measurement and structural models and is suitable for prediction-oriented research involving latent variables measured through multiple indicators.

3.2 Population and Sample

The population of this study consisted of individuals with experience using e-commerce platforms in Indonesia, while the sample comprised 150 respondents selected through purposive sampling based on criteria relevant to the research objectives. Eligible respondents were at least 18 years old, resided in Indonesia, had previously used and completed transactions through e-commerce platforms, had experience providing personal or transactional information, and participated voluntarily. Purposive sampling was applied to ensure that respondents possessed sufficient

experience to assess privacy protection, information security, and user trust. A sample size of 150 respondents was considered adequate for PLS-SEM because the proposed model was relatively simple, involving two exogenous constructs and one endogenous construct, while PLS-SEM is also appropriate for moderate sample sizes and does not require strict multivariate normality assumptions.

3.3 Data Collection

Primary data were collected using a structured questionnaire distributed to respondents who met the predetermined research criteria. The questionnaire consisted of two sections: demographic information covering gender, age, education, occupation, frequency of e-commerce use, and online shopping experience, and measurement items for Privacy Protection Mechanisms, Information Security Policies, and User Trust. All indicators were assessed using a five-point Likert scale ranging from 1 = Strongly Disagree to 5 = Strongly Agree to ensure a consistent and easily understood response format. Before participation, respondents were informed about the academic purpose of the study, participation was voluntary, and personal identities were not included in the analytical dataset to maintain confidentiality and protect respondents' privacy.

3.4 Research Variables

This study consisted of two independent variables and one dependent variable. Privacy Protection Mechanisms (PPM) represented users' perceptions of e-commerce platforms' practices in protecting personal information, including transparency, consent, user control, appropriate data use, confidentiality, and responsible data management. Information Security Policies (ISP) represented users' perceptions of the security measures and procedures used to protect accounts, personal information, and online transactions, including authentication, transaction security, unauthorized access prevention, security monitoring, and incident management. User Trust (UT) served as the dependent variable

and reflected respondents' confidence in the reliability, competence, integrity, and ability of e-commerce platforms to protect user interests and conduct transactions

responsibly. The operational definitions of these variables were developed based on their conceptual characteristics and relevance to the e-commerce context.

Table 1. Operational Variable

Variable	Code	Operational Definition	Main Indicators
Privacy Protection Mechanisms	PPM	Users' perceptions regarding organizational and technological mechanisms implemented by e-commerce platforms to manage and protect personal information responsibly.	Privacy transparency, informed consent, user control, appropriate data use, confidentiality, responsible data sharing
Information Security Policies	ISP	Users' perceptions regarding policies, procedures, and technological safeguards implemented by e-commerce platforms to protect information, accounts, and transactions from security threats.	Authentication, account security, transaction protection, access control, fraud prevention, incident response
User Trust	UT	Users' willingness to rely on an e-commerce platform based on perceptions of its reliability, competence, integrity, and ability to protect users' interests.	Reliability, competence, integrity, confidence, transaction assurance, willingness to rely on the platform

3.5 Data Analysis Technique

Data analysis was conducted using SmartPLS 3 with the Partial Least Squares Structural Equation Modeling (PLS-SEM) approach, consisting of descriptive analysis, measurement model evaluation, structural model evaluation, and hypothesis testing. Descriptive statistics were used to summarize respondent characteristics and responses through frequencies, percentages, means, and standard deviations. The measurement model was evaluated using outer loadings, Cronbach's Alpha, Composite Reliability, Average Variance Extracted (AVE), and discriminant validity through the Heterotrait-Monotrait Ratio (HTMT), with recommended thresholds of ≥ 0.70 for reliability, ≥ 0.50 for AVE, and < 0.90 for HTMT. The structural model was assessed using Variance Inflation Factor (VIF), path coefficients, coefficient of determination (R^2), effect size (f^2), and

predictive relevance (Q^2), where VIF values below 5 indicated acceptable collinearity, R^2 reflected the model's explanatory power, f^2 indicated the contribution of each predictor, and Q^2 values above zero demonstrated predictive relevance. Hypothesis testing was performed through bootstrapping, with relationships considered statistically significant when the t-statistic exceeded 1.96 and the p-value was below 0.05.

4. RESULTS AND DISCUSSION

4.1 Respondent Characteristics

A total of 150 respondents who had experience using e-commerce platforms and conducting online transactions in Indonesia were analyzed. Their characteristics were described based on gender, age, education, occupation, frequency of e-commerce use, and primary platform used.

Table 2. Respondent Characteristics

Characteristic	Category	Frequency	Percentage (%)
Gender	Male	67	44.7
	Female	83	55.3
Age	18–25 years	58	38.7
	26–35 years	52	34.7
	36–45 years	27	18.0
	>45 years	13	8.6

Education	Senior High School	29	19.3
	Diploma	24	16.0
	Bachelor's Degree	78	52.0
	Master's/Doctoral Degree	19	12.7
Occupation	Student	32	21.3
	Private Employee	59	39.3
	Entrepreneur	35	23.3
	Government Employee/Other	24	16.0
E-commerce Usage	<2 times/month	22	14.7
	2–4 times/month	54	36.0
	5–8 times/month	45	30.0
	>8 times/month	29	19.3
Main Platform	Shopee	62	41.3
	Tokopedia	41	27.3
	Lazada	21	14.0
	Blibli	13	8.7
	TikTok Shop/Other	13	8.7
Total		150	100.0

Table 2 shows that the 150 respondents were predominantly female (55.3%) and mostly aged 18–25 years (38.7%), followed by 26–35 years (34.7%). Most respondents held a bachelor's degree (52.0%) and worked as private employees (39.3%). In terms of e-commerce usage, the largest proportion used e-commerce 2–4 times per month (36.0%), followed by 5–8 times per month (30.0%). Shopee was the most frequently used platform (41.3%), followed by Tokopedia (27.3%). These characteristics

indicate that the respondents were largely young, educated, and relatively active e-commerce users, making them relevant for evaluating privacy protection, information security, and user trust in digital transactions.

4.2 Descriptive Analysis of Research Variables

Descriptive statistics were used to describe respondents' general perceptions regarding Privacy Protection Mechanisms, Information Security Policies, and User Trust.

Table 3. Descriptive Statistics of Research Constructs

Construct	N	Mean	Stdv	Interpretation
Privacy Protection Mechanisms (PPM)	150	4.13	0.61	High
Information Security Policies (ISP)	150	4.19	0.58	High
User Trust (UT)	150	4.16	0.60	High

Table 3 indicates that all research constructs were rated at a high level. Information Security Policies (ISP) recorded the highest mean value of 4.19 (SD = 0.58), followed by User Trust (UT) with a mean of 4.16 (SD = 0.60) and Privacy Protection Mechanisms (PPM) with a mean of 4.13 (SD = 0.61). These results suggest that respondents generally perceived e-commerce platforms as having strong privacy protection and information security practices, accompanied by a high level of user trust.

4.3 Measurement Model Assessment

The measurement model, or outer model, was evaluated to determine whether the indicators used in the study appropriately measured their respective latent constructs. The evaluation included indicator reliability, internal consistency reliability, convergent validity, and discriminant validity.

4.3.1 Outer Loading

Indicator reliability was evaluated based on outer loading values. An indicator

was considered to have satisfactory reliability when its loading exceeded 0.70.

Table 4. Outer Loading Results

Construct	Indicator	Outer Loading	Decision
Privacy Protection Mechanisms	PPM1	0.812	Valid
	PPM2	0.845	Valid
	PPM3	0.831	Valid
	PPM4	0.798	Valid
	PPM5	0.862	Valid
	PPM6	0.824	Valid
Information Security Policies	ISP1	0.821	Valid
	ISP2	0.856	Valid
	ISP3	0.838	Valid
	ISP4	0.873	Valid
	ISP5	0.814	Valid
	ISP6	0.847	Valid
User Trust	UT1	0.834	Valid
	UT2	0.868	Valid
	UT3	0.842	Valid
	UT4	0.879	Valid
	UT5	0.816	Valid
	UT6	0.851	Valid

Table 4 shows that all indicators of Privacy Protection Mechanisms (PPM), Information Security Policies (ISP), and User Trust (UT) have outer loading values ranging from 0.798 to 0.879, exceeding the recommended threshold of 0.70. Therefore, all indicators are considered valid and demonstrate adequate indicator reliability, indicating that each item effectively represents its respective construct and can be retained for further PLS-SEM analysis.

4.3.2 Reliability and Convergent Validity

The construct reliability and convergent validity results show that all variables met the required criteria. Cronbach's Alpha values ranged from 0.909 to

0.922 and Composite Reliability values ranged from 0.929 to 0.939, both exceeding the recommended threshold of 0.70. The AVE values for Privacy Protection Mechanisms (0.687), Information Security Policies (0.709), and User Trust (0.720) were also above 0.50. These results confirm that all constructs demonstrate strong internal consistency and satisfactory convergent validity, indicating that the measurement model is reliable and valid for further analysis.

4.4 Discriminant Validity

Discriminant validity was evaluated using the Heterotrait-Monotrait Ratio. HTMT values below 0.90 indicate that the constructs are empirically distinct.

Table 5. HTMT Discriminant Validity

Construct	PPM	ISP	UT
Privacy Protection Mechanisms (PPM)	—		
Information Security Policies (ISP)	0.743	—	
User Trust (UT)	0.792	0.814	—

Table 5 shows that all HTMT values were below the recommended threshold of 0.90, with PPM–ISP at 0.743, PPM–UT at 0.792,

and ISP–UT at 0.814. These results confirm adequate discriminant validity, indicating that Privacy Protection Mechanisms,

Information Security Policies, and User Trust are empirically distinct constructs within the research model.

4.5 Collinearity Assessment

Table 6. Inner VIF Results

Predictor	Endogenous Construct	VIF	Decision
Privacy Protection Mechanisms	User Trust	1.611	No Collinearity Problem
Information Security Policies	User Trust	1.611	No Collinearity Problem

Table 6 shows that both Privacy Protection Mechanisms and Information Security Policies have VIF values of 1.611, which are well below the recommended threshold of 5.00. This indicates that there is no multicollinearity problem among the predictor variables, allowing both constructs to be included in the structural model for further analysis.

4.6 Structural Model Evaluation

4.6.1 Coefficient of Determination

The R^2 value for User Trust was 0.617, with an adjusted R^2 of 0.612, indicating that Privacy Protection Mechanisms and

Before testing the structural relationships, collinearity among the predictor constructs was evaluated through the Variance Inflation Factor.

Information Security Policies jointly explained 61.7% of the variance in User Trust, while the remaining 38.3% was influenced by other factors outside the model. This result demonstrates that the structural model has moderate to substantial explanatory power and confirms that privacy protection and information security are important determinants of user trust in Indonesian e-commerce platforms.

4.6.2 Effect Size

Effect size was evaluated using f^2 to determine the individual contribution of each exogenous variable to User Trust.

Table 7. Effect Size Results

Relationship	f^2	Interpretation
Privacy Protection Mechanisms → User Trust	0.205	Medium Effect
Information Security Policies → User Trust	0.259	Medium Effect

Table 7 shows that Privacy Protection Mechanisms have an f^2 value of 0.205, while Information Security Policies have an f^2 value of 0.259. Both values indicate a medium effect on User Trust, although Information Security Policies demonstrate a slightly stronger contribution. These findings suggest that both privacy protection and information security play meaningful roles in strengthening user trust in e-commerce platforms.

4.6.3 Predictive Relevance

The Q^2 value for User Trust was 0.428, which is greater than zero and therefore confirms that the structural model has

predictive relevance. This result indicates that Privacy Protection Mechanisms and Information Security Policies provide meaningful predictive information in explaining User Trust in e-commerce platforms.

4.7 Hypothesis Testing

Hypothesis testing was conducted using the bootstrapping procedure in SmartPLS 3. A hypothesis was considered supported when the path coefficient was positive, the t-statistic exceeded 1.96, and the p-value was below 0.05.

Table 8. Direct Effect and Hypothesis Testing

Hypothesis	Relationship	Original Sample (β)	Std. Deviation	t-Statistic	p-Value	Decision
H1	PPM → UT	0.412	0.070	5.886	<0.001	Supported

H2	ISP → UT	0.463	0.071	6.521	<0.001	Supported
----	----------	-------	-------	-------	--------	-----------

Table 8 shows that both hypotheses are supported. Privacy Protection Mechanisms have a positive and significant effect on User Trust ($\beta = 0.412$, $t = 5.886$, $p < 0.001$), while Information Security Policies also have a positive and significant effect on User Trust ($\beta = 0.463$, $t = 6.521$, $p < 0.001$). The larger coefficient of Information Security Policies indicates that security policies have a slightly stronger influence on User Trust than privacy protection mechanisms.

Discussion

The results confirm that Privacy Protection Mechanisms (PPM) have a positive and significant effect on User Trust (UT) in e-commerce platforms, supporting H1. This finding indicates that stronger privacy protection increases consumers' confidence in e-commerce platforms. Transparent data collection practices, appropriate consent procedures, user control, confidentiality, and responsible third-party data sharing can reduce uncertainty regarding the management of personal information. This is particularly important because consumers disclose various forms of personal and transactional data while having limited ability to directly monitor how such information is subsequently processed [1], [2]. The highest outer loading for PPM was recorded by PPM5 (0.862), indicating that confidentiality protection is particularly important in shaping users' perceptions of privacy protection.

The effect size of PPM on User Trust was moderate ($f^2 = 0.205$), demonstrating that privacy protection makes a meaningful contribution to trust formation. From the perspective of structural assurance, effective privacy mechanisms provide formal safeguards that reduce consumers' perceived vulnerability and signal organizational integrity. In the Indonesian e-commerce context, these findings emphasize that privacy governance should extend beyond regulatory compliance and become an integral part of customer relationship management [9], [34]. E-commerce platforms should therefore

maintain transparent privacy policies, obtain appropriate consent, minimize unnecessary data collection, provide accessible privacy controls, maintain confidentiality, and clearly communicate third-party data-sharing practices.

Information Security Policies (ISP) also have a positive and significant effect on User Trust, supporting H2. ISP emerged as the stronger predictor of User Trust compared with PPM, with a higher path coefficient and effect size ($f^2 = 0.259$). This result indicates that authentication systems, secure payments, transaction verification, fraud prevention, access controls, and incident response mechanisms can strengthen consumers' confidence in e-commerce platforms [35], [36]. The stronger influence of ISP may reflect the direct consequences associated with security failures, including unauthorized transactions, account takeover, payment fraud, and compromised credentials. ISP4 recorded the highest outer loading (0.873), suggesting that preventing unauthorized access is particularly important in shaping users' perceptions of platform security.

These findings are consistent with structural assurance theory because consumers cannot directly evaluate the technical security architecture of e-commerce platforms and therefore rely on observable security mechanisms as indicators of platform competence and reliability. Authentication, transaction confirmation, login alerts, device verification, and suspicious activity notifications can provide visible evidence that platforms actively protect users and their transactions. Consequently, e-commerce providers should continuously strengthen authentication, access control, encryption, transaction monitoring, fraud detection, vulnerability management, and incident response capabilities. Overall, both privacy protection and information security contribute meaningfully to User Trust, although information security demonstrates a relatively stronger influence, emphasizing the importance of integrating privacy governance

and cybersecurity management in building sustainable consumer trust.

Theoretical Implications

The findings support the role of structural assurance in explaining trust formation in digital commerce, as both Privacy Protection Mechanisms and Information Security Policies significantly reduce uncertainty in online transactions. The significant effect of Privacy Protection Mechanisms on User Trust indicates that trust is influenced by perceptions of organizational integrity in managing personal data, while the significant effect of Information Security Policies shows that technological and organizational competence in protecting accounts and transactions also strengthens trust. Importantly, the study confirms that privacy protection and information security should be treated as distinct constructs rather than combined into a single security dimension, as both independently influence User Trust with coefficients of 0.412 and 0.463, respectively. This demonstrates that privacy governance and security governance represent complementary but empirically distinguishable foundations of digital trust.

Practical Implications

From a managerial perspective, the findings indicate that e-commerce providers should integrate privacy governance and information security management to strengthen user trust. Platforms need to provide clear information about data collection, usage, retention, and sharing, while also giving users accessible control over consent, privacy settings, and personal data. At the same time, companies should

strengthen authentication, account protection, transaction monitoring, fraud detection, and secure payment systems to reduce security risks. Transparent and responsive incident-handling procedures are also essential because timely communication and effective corrective actions can help maintain consumer confidence when security problems occur.

5. CONCLUSION

This study concludes that Privacy Protection Mechanisms and Information Security Policies are important determinants of User Trust in e-commerce platforms in Indonesia. Users are more likely to trust platforms that manage personal data transparently, responsibly, and confidentially while providing strong protection for accounts and transactions. Information security appears to play a particularly important role through authentication, transaction protection, fraud prevention, and unauthorized access controls. From a practical perspective, e-commerce providers should integrate privacy governance and information security into their digital management strategies by strengthening transparency, consent mechanisms, personal data controls, authentication systems, secure payments, fraud detection, and incident response. Privacy and security should also be managed as complementary but distinct dimensions of trust. Future research may expand the model by examining other factors such as perceived risk, platform reputation, service quality, customer satisfaction, digital literacy, and transaction experience across broader and more diverse samples.

REFERENCES

- [1] D. Astria and M. Santi, "Pemanfaatan Aplikasi Whatsapp Bisnis Dalam Strategi Pemasaran Online Untuk Meningkatkan Jumlah Penjualan," ... *Ekon. Syari'ah & Bisnis Islam* ..., 2021.
- [2] B. Li, T. Zhang, N. Hua, and Y. Wang, "A dynamic model of crisis management from a stakeholder perspective: the case of COVID-19 in China," *Tour. Rev.*, 2021, doi: 10.1108/TR-09-2020-0413.
- [3] L. N. Auliani, "Implementasi Enterprise Resource Planning Odoo dalam Optimalisasi Proses Bisnis PT XYZ," *Qualitative Res. Bus. Soc. Sci.*, vol. 1, no. 1, pp. 50–61, 2023.
- [4] R. Sholeh and K. Huda, "Pengaruh Kemajuan Teknologi Terhadap Volume Pejualan Ritel Di Kota Mojokerto," *Optima*, vol. 3, no. 1, 2019, doi: 10.33366/optima.v3i1.1253.
- [5] R. R. Firman, "Kajian Relasi Antara Public Figure Dan Jingle Tvc Terhadap Minat Beli Konsumen (Studi Kasus: Iklan Shopee 'Sepedaku Mana' Tahun 2017)," *J. Kreat. Desain Prod. Ind. dan Arsit.*, vol. 6, no. 1,

- 2020, doi: 10.46964/jkdpia.v6i1.32.
- [6] D. A. P. Sari, I. Febrilia, A. Kresnamurti, P. D. Dirgantari, and H. Rachmahani, "Why do people shop? Understanding consumer e-commerce shopping intention in Indonesia: Mediating effect of shopping orientation," *Nurture*, vol. 17, no. 2, pp. 81–92, 2023.
 - [7] G. N. Sumahir, H. Wahyudi, and T. Nirmala, "The Effect of Research and Development (R&D) Investment, E-Commerce Company Employee, and E-Commerce Transaction Volume on Economic Growth in Indonesia 2010Q1–2020Q4," *Perad. J. Econ. Bus.*, vol. 1, no. 2, pp. 9–18, 2022.
 - [8] R. N. Anwar and A. Afifah, "Pengaruh Kepercayaan dan Keamanan Konsumen terhadap Minat Beli di situs Online (Studi Kasus pengunjung situs Lazada di Jakarta Timur)," *J. Manaj.*, vol. 9, no. 1, p. 46, 2018, doi: 10.32832/jm-uika.v9i1.1316.
 - [9] F. Fernaldo and R. Oktavianti, "Pengaruh Daya Tarik Iklan E-commerce terhadap Brand Trust Konsumen (Survei terhadap Penonton Iklan Tokopedia #MulaiAjaDulu di Youtube)," *Prologia*, vol. 4, no. 2, p. 316, 2020, doi: 10.24912/pr.v4i2.6515.
 - [10] E. Moriuchi and I. Takahashi, "An empirical study on repeat consumer's shopping satisfaction on C2C e-commerce in Japan: the role of value, trust and engagement," *Asia Pacific J. Mark. Logist.*, vol. 35, no. 3, pp. 560–581, 2023.
 - [11] M. Bala and D. Verma, "A Critical Review of Digital Marketing Paper Type: - Review and Viewpoint," *Int. J. Manag. IT Eng.*, vol. 8, no. 10, pp. 321–339, 2018.
 - [12] B. Sivathanu, "Enhancing the customer's experience in a digital world: An empirical study," *Int. J. Appl. Bus. Econ. Res.*, vol. 15, no. 22, pp. 487–495, 2017.
 - [13] S.-C. Necula, "Exploring the Impact of Time Spent Reading Product Information on E-Commerce Websites: A Machine Learning Approach to Analyze Consumer Behavior," *Behav. Sci. (Basel)*, vol. 13, no. 6, p. 439, 2023.
 - [14] N. Chawla and B. Kumar, "E-Commerce and Consumer Protection in India: The Emerging Trend," *J. Bus. Ethics*, vol. 180, no. 2, pp. 581–604, 2022, doi: 10.1007/s10551-021-04884-3.
 - [15] E. Satryawati, "Pengaruh Kepercayaan Dan Kepuasan Terhadap Loyalitas Pelanggan E- Commerce," *J. Teknol. Inform. dan Komput.*, vol. 4, no. 1, pp. 36–52, 2018, doi: 10.37012/jtik.v4i1.284.
 - [16] J. Billanes and P. Enevoldsen, "A critical analysis of ten influential factors to energy technology acceptance and adoption," *Energy Reports*, vol. 7, pp. 6899–6907, 2021, doi: <https://doi.org/10.1016/j.egyr.2021.09.118>.
 - [17] D. Kala, D. S. Chaubey, R. K. Meet, and A. S. Al-Adwan, "Impact of user satisfaction with e-government services on continuance use intention and citizen trust using TAM-ISSM framework," *Interdiscip. J. Information, Knowledge, Manag.*, vol. 19, p. 1, 2024.
 - [18] O. Kibik, O. Taran-Lala, V. Saienko, T. Metil, and ..., "Strategic Vectors for Enterprise Development in the Context of the Digitalization of the Economy," *Postmod. ...*, 2022.
 - [19] R. H. Binsaeed, Z. Yousaf, A. Grigorescu, A. Samoila, R. I. Chitescu, and A. A. Nassani, "Knowledge Sharing Key Issue for Digital Technology and Artificial Intelligence Adoption," *Systems*, vol. 11, no. 7, 2023, doi: 10.3390/systems11070316.
 - [20] E. Tria Wahyuningtilhas, Y. Giri Sucahyo, and A. Gandhi, "Driving Factors for MSMEs in Indonesia to Adopt Information Technology on Culinary," in *Proceedings of the 5th International Conference on E-Commerce, E-Business and E-Government*, 2021, pp. 79–84.
 - [21] P. Sukmasetya, T. Haryanto, F. A. Sadewi, R. B. G. Maulida, H. S. Aliudin, and B. Sugiarto, "Pemanfaatan Digital Marketing sebagai Media Pemasaran Global untuk Meningkatkan Penjualan Produksi pada Home Industry," *Community Empower.*, vol. 5, no. 2, pp. 28–35, 2020, doi: 10.31603/ce.v5i2.3514.
 - [22] M. B. Gulfraz, M. Sufyan, M. Mustak, J. Salminen, and D. K. Srivastava, "Understanding the impact of online customers' shopping experience on online impulsive buying: A study on two leading E-commerce platforms," *J. Retail. Consum. Serv.*, vol. 68, no. March, p. 103000, 2022, doi: 10.1016/j.jretconser.2022.103000.
 - [23] K. X. Wong *et al.*, "Shopee: How Does E-commerce Platforms Affect Consumer Behavior during the COVID-19 Pandemic in Malaysia?," *Int. J. Account. Financ. Asia Pasific*, vol. 6, no. 1, pp. 38–52, 2023.
 - [24] S. Yuniarti, "Perlindungan Hukum Data Pribadi Di Indonesia," *Bus. Econ. Commun. Soc. Sci. J.*, vol. 1, no. 1, pp. 147–154, 2019, doi: 10.21512/becossjournal.v1i1.6030.
 - [25] M. Fenwick, M. C. Compagnucci, H. Haapio, and E. P. M. Vermeulen, "Integrating Law, Technology and Design: Teaching Data Protection & Privacy Law in a Digital Age," 2021.
 - [26] M. Humayun, N. Z. Jhanjhi, M. Alruwaili, and ..., "Privacy protection and energy optimization for 5G-aided industrial Internet of Things," *IEEE ...*, 2020.

- [27] A. Derossi, B. Bhandari, K. van Bommel, M. Noort, and C. Severini, "Could 3D food printing help to improve the food supply chain resilience against disruptions such as caused by pandemic crises?," *Int. J. Food Sci. Technol.*, vol. 56, no. 9, pp. 4338–4355, 2021, doi: 10.1111/ijfs.15258.
- [28] B. Wirajovi Aulia, M. Rizki, and P. Prindiyana, "Peran Krusial Jaringan Komputer dan Basis Data dalam Era Digital," *J. Sist. Inf. dan Teknol. Informasi*, vol. 1, no. 1, pp. 9–20, 2023, doi: 10.33197/justinfo.vol1.iss1.2023.1253.
- [29] V. V Timchenko, S. Y. Trapitsin, and Z. V Apevalova, "Educational technology market analysis," in *2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, IEEE, 2020, pp. 612–617.
- [30] R. Raihani, M. Iskandar, L. Prihatin, and R. Hendra, "Determinant Factor Analysis of Financial Performance of Micro, Small and Medium Enterprises with Social Capital as a Moderating Variable during COVID-19 in Aceh, Indonesia," *Stud. Bus. Econ.*, vol. 19, no. 2, pp. 176–198, 2024, doi: 10.2478/sbe-2024-0032.
- [31] R. Yang, *Algorithms for Data-Driven Business Intelligence with Applications to Revenue Optimization and Financial Forecasting*. search.proquest.com, 2019.
- [32] S. Liu, L. Hou, X. Chen, M. Huang, and H. Hu, "Digital Transformation and Innovation Performance of High-Tech SMEs: Evidence from the Internet Big Data," in *Proceedings of the 2021 3rd International Conference on E-Business and E-commerce Engineering*, 2021, pp. 62–66.
- [33] H. Ma and X. Zhang, "Construction of smart marketing model of agricultural products E-commerce in the era of big data," *Mob. Inf. Syst.*, vol. 2022, pp. 1–10, 2022.
- [34] N. Nofrizal *et al.*, "Can Product Quality Improve Purchase Decisions in E-Commerce and Social Media through Customer Loyalty and Trust?," *Binus Bus. Rev.*, vol. 14, no. 2, pp. 147–161, 2023.
- [35] Q. Liu, H. Jiang, and Y. Chen, "Research on the Construction of Consumer Trust Relationship Based on Cross-border E-commerce Platform," in *Proceedings of the 8th International Conference on Industrial and Business Engineering*, 2022, pp. 39–45.
- [36] S. Ling, C. Zheng, and D. Cho, "How Brand Knowledge Affects Purchase Intentions in Fresh Food E-Commerce Platforms: The Serial Mediation Effect of Perceived Value and Brand Trust," *Behavioral Sciences*, vol. 13, no. 8, 2023. doi: 10.3390/bs13080672.